

Safeguard PDF Portable USB Security

Product Manual for Windows

Version 1.0

Revision 1.14



Table of Contents

CHAPTER 1: INTRODUCTION	4
1.1.1 Features	5
1.1.2 Benefits.....	6
CHAPTER 2: ITEMS TO CONSIDER	8
2.1.1 USB Devices supported	8
2.1.2 Read-only Devices	8
2.1.3 Execute Rights.....	8
2.1.4 Offline Use	9
2.1.5 Offline Use & Document Expiry	9
2.1.6 Offline Use & Restrict IP	9
2.1.7 Watermarking & Dynamic Variables.....	10
2.1.8 Operating Systems Supported	10
CHAPTER 3: USING SAFEGUARD PDF PORTABLE	11
3.1 INSTALLATION	11
3.2 PRE-REQUISITES	12
3.2.1 Safeguard Viewer	12
3.2.2 Autorun app & FAT32.....	12
3.3 PROTECT TO USB APPLICATION	13
3.3.1 Publishing PDC Documents & Keystores	14
3.3.1.1 Secure Viewer	16
3.3.1.2 Autorun Interface	17
3.3.2 Publishing Blank Keystores.....	19
3.3.3 Producing larger volumes of secure USB devices	20
CHAPTER 4: ADMINISTERING USB DEVICES	21
4.1.1 Managing USB devices	21
4.1.1.1 USB ID.....	23
4.1.1.2 Name, Email & Company.....	23
4.1.1.3 Notes	23
4.1.1.4 Status	23
4.1.1.5 Start Date	23
4.1.1.6 Restrict IP	23
4.1.1.7 Set Publication & Document Access	24
4.1.1.8 Change number of Views & Prints.....	24
4.1.1.9 Batch Changes	24
4.1.2 Exporting USB records	25
4.1.2.1 Export.....	25
4.1.2.2 Format.....	25
CHAPTER 5: SECURE USB VIEWER	27

5.1.1	Opening Secure Documents	27
5.1.1.1	Using the Autorun application	27
5.1.1.2	Associating the Viewer software with PDC files	28
5.1.2	Keystore Password Protection	28
5.1.2.1	Set Password	29
5.1.2.2	Change or Remove Password	29
5.1.3	Remove Keystore	30
5.1.4	USB ID	30
5.1.5	Program Updates	31
CHAPTER 6: FAQs & SUPPORT ISSUES		32
6.1.1	Do I have to re-protect my PDF files in order to use them with USB devices?	32
6.1.2	Do users have to download new documents to their USB devices or can they open them from their hard disk?	32
6.1.3	Do users have to connect to a licensing server to register?	32
6.1.4	My documents connect to the Internet every time to verify access. How will they work with a USB Device?	32
6.1.5	How do dynamic watermarks work with USB devices?	33
6.1.6	I have protected some documents to a USB device but I want users to download additional documents in the future. How will this work?	33
6.1.7	How can I make sure users only open secure documents from their work location?	34
6.1.8	A user has forgotten their keystore password. What can I do?	34
6.1.9	My USB devices were distributed by a third party. How do I identify a USB device with a user?	34
6.1.10	How can I protect content on USB devices whilst being sent by postal mail?	34
6.1.11	Error Message: Error loading component, cannot find one or more components	35
6.1.12	Why do I get an Aborted error when the Secure Viewer is being written to USB?	35
6.1.13	Error Message: Windows cannot access the specified device, path, or file	36
6.1.14	Error Message: Error opening keystore file	36
6.1.15	Error: The 'Protect to USB' application either does not load, or takes a long time to load	36
6.1.16	Error: The 'Protect to USB' application hangs when protecting to USB devices	37



Chapter 1: Introduction

Safeguard PDF Portable is a portable, no installation Viewer and secure PDF document solution for USB devices (USB sticks). It can be used as a completely offline solution (no Internet access required), and since secure documents are locked to USB devices rather than to specific computers they can be used anywhere.

Safeguard PDF Portable provides real security without the installation overheads - nothing is loaded onto or installed in anything on the user's computer system. The PDF USB Secure Viewer software runs directly from the USB device, working in exactly the same way as the Viewer that requires installing on a computer.

Publishers purchasing Safeguard PDF Portable for USB can distribute secure Viewers, documents, and keystores on USB devices, offering publishers and users novel and significant flexibility in both distributing and using DRM controlled documents. For example, digital editions can now be sold over the counter without the publisher needing to know anything about the customer, just like a normal book. And users with roaming profiles can readily use secured information since the USB is taken with them from computer to computer.

Safeguard PDF Portable resolves issues of firewall access, granting administrator privileges, Internet availability, and the use of roaming profiles. It does not rely on insecure plug-ins, self-extracting exes, JavaScript, or Flash, in order to provide total copy protection. For additional user privacy, USB devices can be password locked to prevent unauthorized use if lost or stolen.



NOTE: This manual has been created as a supplement to the Safeguard/Enterprise Writer manual to address features and functions specific to Safeguard PDF Portable. It is assumed that the reader is already fully conversant with all the content of the Safeguard/Enterprise Writer manual and therefore references in this manual are assumed to be fully understood.

1.1.1 Features

- Viewer application and keystore is pre-loaded so nothing is installed on the recipient PC.
- Does not require for the user to be identified or the registration tracked - avoids the use of personally identifiable information (PII).
- Users never have to connect to the Internet - users don't have to connect to a licensing server to register, to obtain access rights, or to view documents.
- USB devices may be pre-loaded with both authorized and un-authorized documents but licensed piecemeal (so publishers can protect thousands of documents to USB and license individual users to access selected documents after distribution).
- Additional documents may be added to USB devices online (including revisions).
- USB devices may be pre-loaded with just the Viewer and a pre-registered keystore – so that users can download documents online at a later date and publishers can grant access to them as and when they are purchased.
- Possession of the USB device is the grant of rights, so the USB device may be lent or re-sold just like an ordinary book (but the controls cannot be copied).
- USB documents can be controlled in both online and offline modes.
- Publishers can set up 'standard' contents lists for USB devices, and then create multiple USBs on-the-fly.
- Existing secured PDF documents are copied across to the USB devices so publishers do not have to re-protect documents specifically for PDF USB Security.
- Existing PDF structures and controls are maintained on documents secured to USB.
- You do not need a pre-established link between the publisher and the user, the publisher can license and issue USB content without having to create a user first.

- Existing users can also be extended to use Safeguard PDF Portable quickly and easily.
- The first truly zero installation secure PDF DRM system available - no downloads, no plug-ins to install, no JavaScript or Flash risks, no self-extracting exes to run, no applications to install.
- Users can password protect USB devices so that loss or theft of a USB device does not result in secure documents being used by unauthorized users.
- USB devices can be locked to specific IP address ranges (e.g. to prevent corporate users taking USB devices home to use secure documents there).
- No need to purchase special hardware for USB duplication. Just plug any manufacturer's USB device into your computer.

1.1.2 Benefits

- Viewer application and keystore is pre-loaded so nothing is installed on the recipient PC.
- Saves time and money - IT departments don't have to custom install, assign administrator privileges, or carry out formal evaluation.
- Truly portable solution - protected PDF documents are locked to the USB device rather than individual computers so they can be used on any computer, anywhere.
- Complete offline solution – documents can be used without mandatory use of the Internet when this may be forbidden for security reasons.
- No licenses for users to register - publishers don't need to go through the process of setting up user records.
- No firewall issues - documents and keystores are distributed on USB devices without end users ever having to connect to the Internet to register, download decryption keys, or verify access (you can of course enforce document access verification if you want to and have users download additional secure documents).

- Allows users with roaming profiles to use secure documents immediately.
- Enables students to take their own 'library' of secure PDF documents with them from class to class and also back home.
- Digital editions can now be sold over the counter without the publisher needing to know anything about the customer, just like a normal book.
- Secure documents are instantly accessible just like ordinary files.
- The same secure PDF Viewer is used for both Windows and USB (the normal Safeguard PDF Viewer is used, not a 'lite' version) ensuring consistent delivery of features and functionality.
- The full strength of secured PDF documents without the complications.



Chapter 2: Items to Consider

Before using Safeguard PDF Portable please consider the following points as they may affect your protection strategy approach.

2.1.1 USB Devices supported

Safeguard PDF Portable only supports USB sticks (USB memory stick, USB token, USB flash device, USB flash drive, external USB hard drive or SSD) and does NOT support other types of flash memory devices (for example: SD, SDHC, XD, MMC, MD, MSPD, Compact Flash (CF), or SmartMedia cards). Whilst these devices may be displayed in the Safeguard Portable application, you should NOT select them because licenses are tied to your physical hardware rather than the media that you insert. Secure documents protected to non-USB devices will therefore only work on the computer where they were protected.

2.1.2 Read-only Devices

Make sure the USB device is not marked as read-only UNLESS you are certain that you do not want users to be able to download new documents from the web to view on their USB device.

Also, if you have set document expiry in days for an offline document (one that does not have to connect to the server to verify), then it will not work because the Viewer must be able to write date control information to the keystore in order to update it.

2.1.3 Execute Rights

Some companies prevent users running executable files on USB devices. Since Safeguard PDF Viewer runs as an EXE file on the USB device it must be allowed to run on the machines where it is to be used.

2.1.4 Offline Use

Whilst Safeguard PDF Portable can be used in offline mode (no server connection is required when opening documents for the first time if a **populated keystore** has been stored on the USB device) please remember that any of the following options requires (and enforces) a server connection:

- Document logging
- Limited prints (server connection required at print time)
- Limited views
- Verify document access = each time the document is opened
- Verify document access = every n days
- Verify document access = after n days and then never again

2.1.5 Offline Use & Document Expiry



NOTE: If you want to make use of document expiry in **days** (not a fixed date), then make sure that documents **verify with the server** on a regular basis.

If you allow offline document use, users can remove their keystores in order to start the count again. This happens because the Viewer does not have to connect to a server to obtain the decryption key and date for the document, so the first open date is only recorded locally on the USB device and is not checked against a server.

2.1.6 Offline Use & Restrict IP



NOTE: If you want to restrict use of USB devices to specific IP addresses or address ranges (Safeguard Enterprise only) then you must make sure that documents **verify with the server**. This is because the IP address range is verified against a server record.

2.1.7 Watermarking & Dynamic Variables

By default, the USB ID is displayed in the Name field on the administration system, and so this information is used as the username in dynamic watermarking. If you want to associate a particular user with a USB device then you need to edit the name, company, and email fields for each USB device on the administration system so that this information is displayed instead.

2.1.8 Operating Systems Supported

Safeguard PDF Portable and USB Viewer are currently only available for the Windows Operating System.



3.1 Installation

Safeguard PDF Portable is included as part of the Writer installation (Safeguard version 3.0.10 and above, and Enterprise 4.0.12 and above). If you have purchased Safeguard PDF Portable then an additional option off the Writer program menu 'Protect to USB' becomes available as shown below.

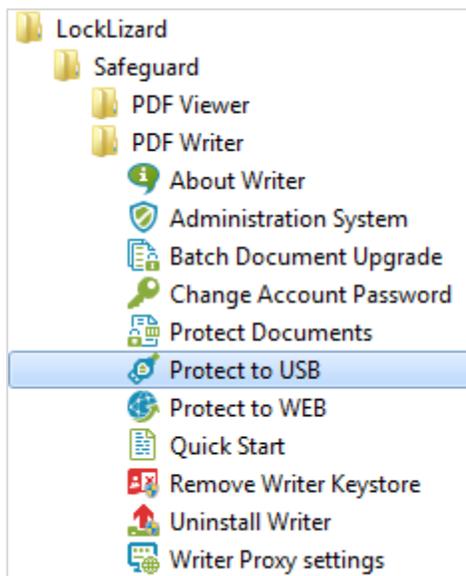


Diagram 1: Protect to USB option

If you have Safeguard version 3.0.10 or above or Enterprise 4.0.12 or above already installed you will need to remove your Writer Keystore (use the Remove Writer Keystore option from the Windows Start menu > Locklizard program group) and re-register to activate the new functionality.

If you need to install a newer version of the Writer software that supports Safeguard PDF Portable, then you need to de-install your current version of Safeguard Writer or Enterprise Writer first. Remove your Writer Keystore (use

the Remove Writer Keystore option from the Windows Start menu > Locklizard program group) AND then de-install the Writer software (use the Uninstall Writer option from the Locklizard program group) if necessary. You can then download and install the appropriate Writer from the Locklizard web site and re-register your Writer license.

3.2 Pre-requisites

3.2.1 Safeguard Viewer

Assuming you want to publish the Safeguard Viewer to USB:

1. The Viewer must be installed on the computer that you are publishing PDC files to USB on.
2. The Viewer must be installed in the default location - C:\Program Files\Locklizard Safeguard PDF Viewer.
3. The Viewer must be installed using the installation option 'complete install'. This installs both 32 and 64 bit versions of the Viewer, includes all language files, and the autorun application.
4. You must use the EXE installation and not the MSI one.
5. If you want to include the **v3** Viewer on USB, then Safeguard 4.024 or Enterprise 5.0.43 or above must be installed.

3.2.2 Autorun app & FAT32

USB sticks must be formatted as FAT32 if you want to include the autorun application (the GUI to display the files available on the USB device).

If the drive is formatted as NTFS then no files will be displayed in the autorun application.

3.3 Protect to USB Application

Select the 'Protect to USB' option from the Windows Start menu > Programs > Locklizard menu to run the application.

The following GUI is displayed:

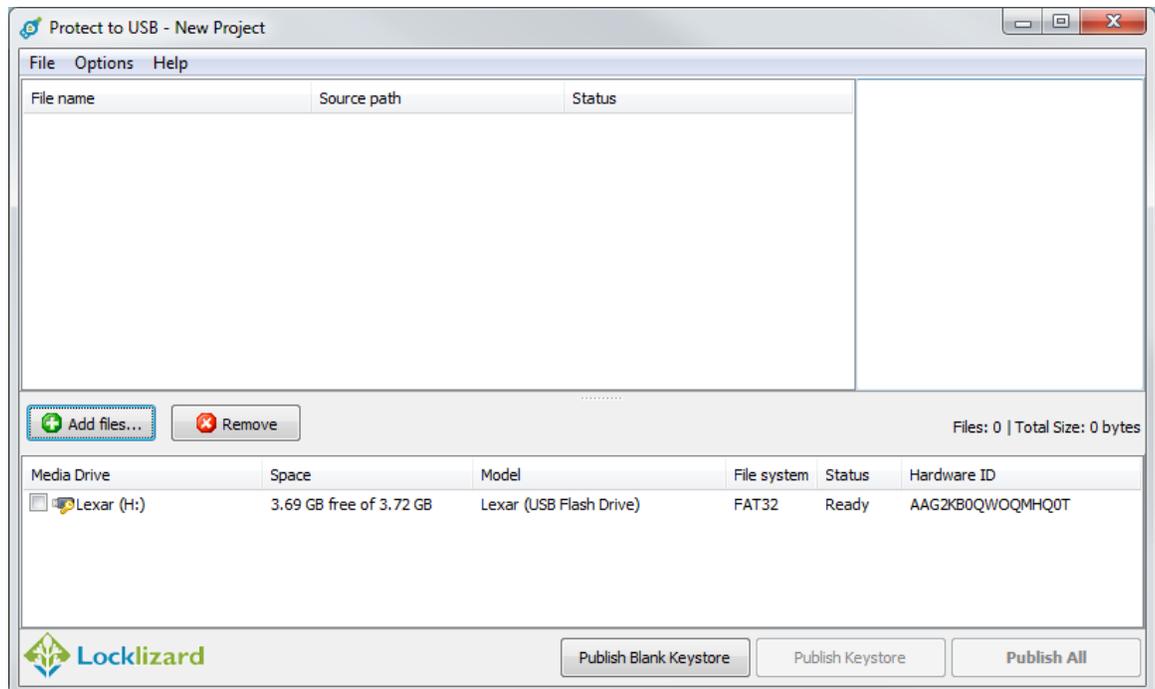
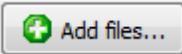


Diagram 2: Safeguard PDF Portable GUI

From here you can choose to create a blank keystore (pre-registered) on the USB device, create a keystore populated with decryption keys, or publish both documents and decryption keys. You can also choose whether you want to include the Viewer software and an Autorun interface (used to open PDC files on the USB device).

If you are not distributing secured documents on the USB device please go directly to section 3.3.2 of this manual.

3.3.1 Publishing PDC Documents & Keystores

1. Select the  button to bring up a browse dialog which allows you to choose the PDC files you want to lock to the USB device.



NOTE: You cannot protect PDF files directly onto USB devices, you can only select existing protected (PDC) documents. You cannot change the controls already applied to these PDC documents at this time.

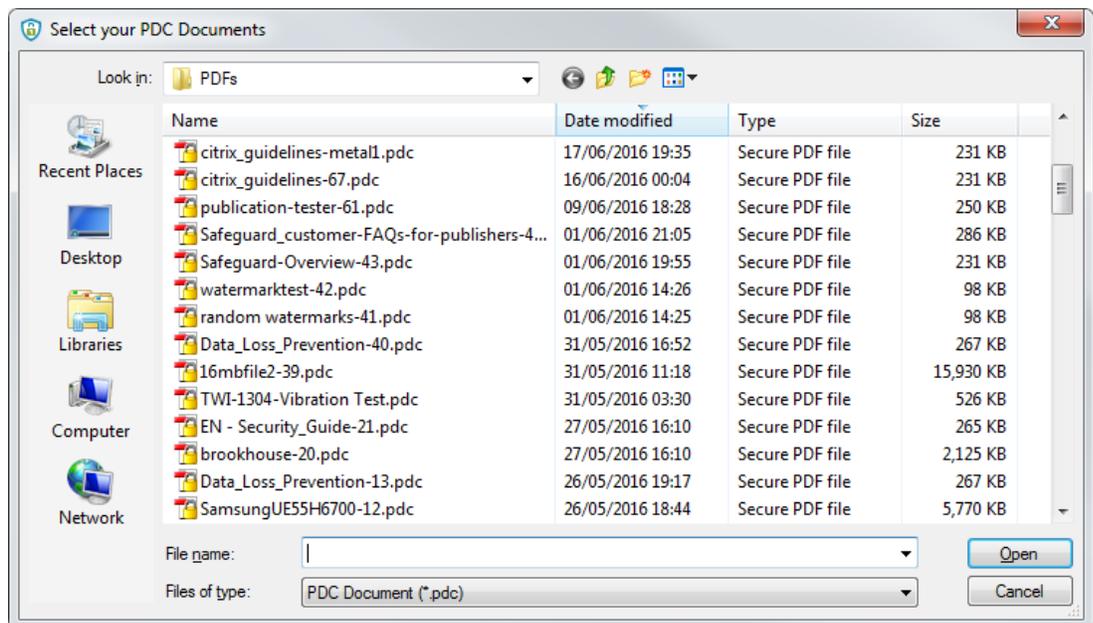
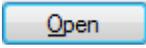


Diagram 3: Add files dialog

Once you have selected your PDC files press the  button to add them.

The Safeguard Portable GUI is then updated with the files you have added, as shown below:

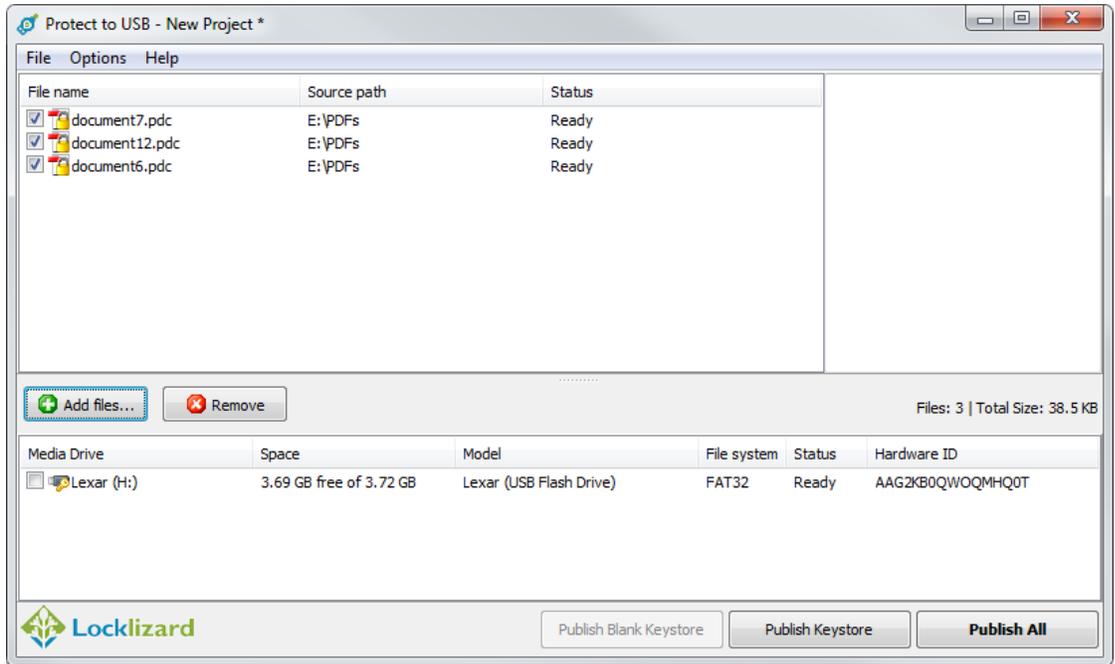


Diagram 4: Add files dialog

Select a file by clicking on it and you will see its protected document properties in the right-hand pane.

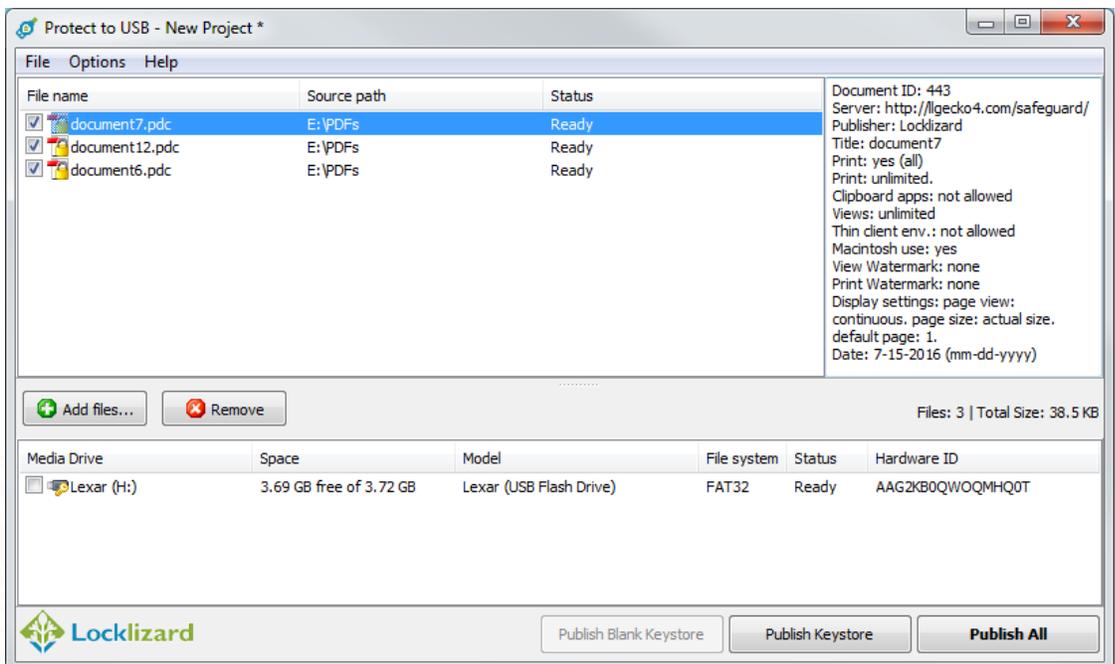


Diagram 5: File Properties

If you decide to not include some of the files you have previously selected then you can either remove them by highlighting them and pressing the



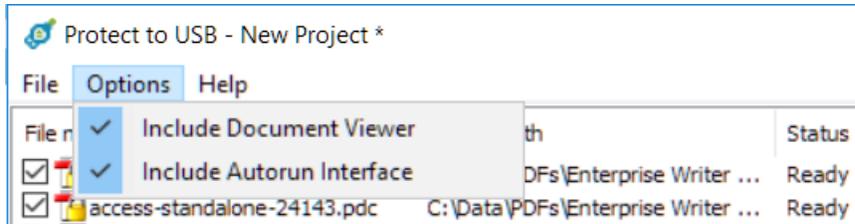
button, right-clicking on the files to bring up a menu selection, or by unchecking the boxes next to the file name(s).

Alternatively, just uncheck the boxes next to the documents you do not want to include on the USB.

2. If you have not already done so, plug in the USB device(s) that you want to lock the PDC documents to. These are then shown in the Media Drive section. Check the boxes next to the USB device(s) that you want to use.

If any of the USB devices that you plug in show their status as invalid, this means that either the device cannot be read or the hardware ID cannot be retrieved from the device, and the device cannot be used.

3. From the **Options menu** select whether you want to include the **Secure Viewer** on the USB device (Include Document Viewer) and if you want to include the **Autorun Interface**.



3.3.1.1 Secure Viewer

Checking the Document Viewer installs the Secure Viewer application software on the USB device, allowing users to view documents from the USB without having to install the Secure Viewer on their computer.



NOTE: If you want to include the Secure Viewer then you must make sure that the Viewer application is installed correctly. See [Installation Pre-requisites](#).

You may decide not to include the Document Viewer if you are using the USB device purely to distribute documents and their associated keystores where users already have the Secure Viewer software installed on their computers (say a corporate installation) but access to the Internet is not allowed so that documents and keystores need to be distributed on USB before they can be viewed.

3.3.1.2 Autorun Interface

Including the Autorun interface enables users to run a file called 'View Documents.exe' which displays a dialog showing all the protected documents available on the USB device. Users can then select from this dialog the documents they wish to view, as shown below:

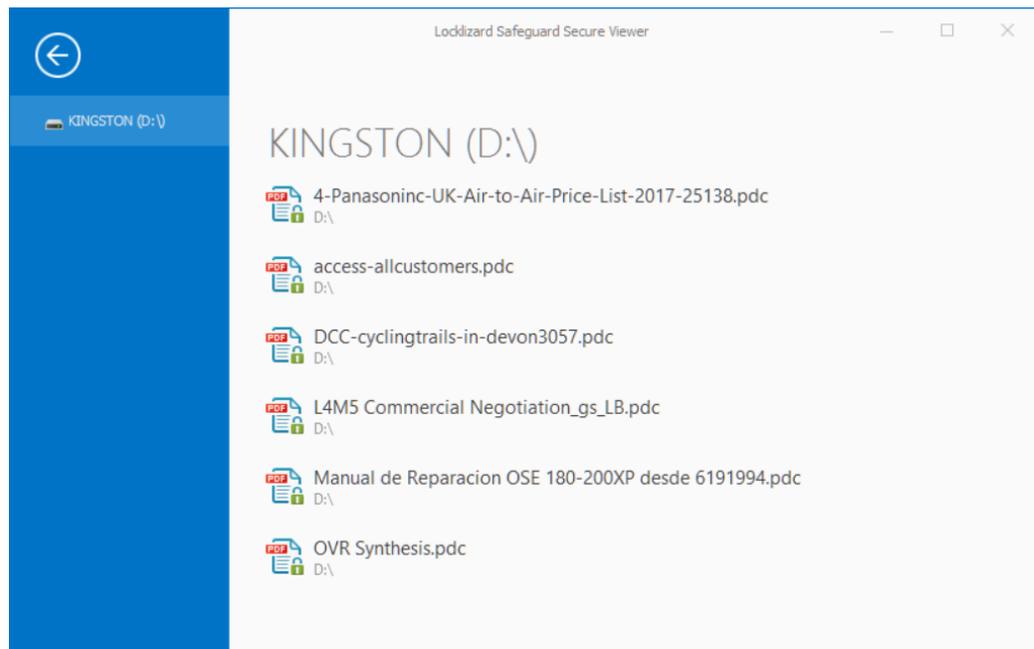
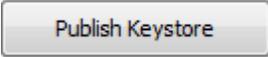


Diagram 6: Autorun Interface (Safeguard v3 Viewer)

You may decide not to include the Autorun interface if users have installed the Secure Viewer software on their computers, or if you plan to bundle your own interface for the selection of PDC documents. If Autorun is not included and no Viewer is installed on the machine, the user will have to manually load the Secure Viewer (by double-clicking on the PDCViewer64.exe application in the Viewer folder) and open the documents from there.

4. Select either the  button or the  button depending on whether you want to publish a pre-registered keystore populated with decryption keys (Publish Keystore) for the selected documents, or a pre-registered keystore and documents (Publish All), to the USB device.

You might want to publish a keystore to a USB device without any documents if you have protected documents to Publications and you want users to be able to download the latest documents from your web site but have the keys available to view them from the USB device.



NOTE: By publishing a keystore (Publish Keystore) or a keystore and documents (Publish All) you do NOT have to assign document/publication access on the administration system for the USB device, since decryption keys for the selected documents are already available on the USB device.

On pressing either button a progress dialog is displayed:

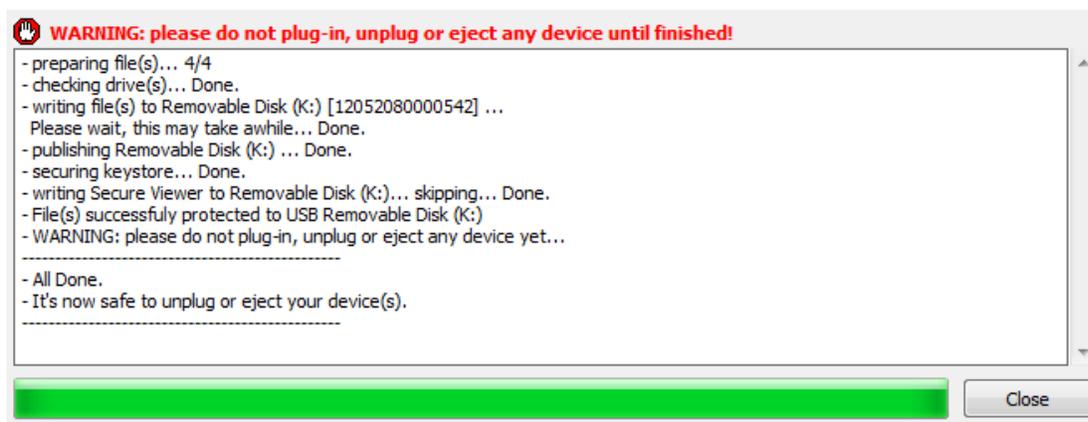


Diagram 7: Progress Dialog

The 'All Done' message is displayed once the process is complete.



NOTE: Any invalid PDC files are skipped (not processed). An invalid document for example could be one that you still have the PDC file for on disk but have deleted the corresponding document record from the admin system.

5. If you plan to write the same documents/keystores to other USB devices in the future then it is convenient to save this as a project. To do this, from the File menu, select the option 'Save Project'. You can then open this project at a later date (File menu > 'Open Project') with your documents already loaded.

3.3.2 Publishing Blank Keystores

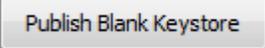
Publishing a blank keystore creates a keystore that is pre-registered - locked to both you as a publisher and the USB device itself. So although there are no decryption keys currently in the keystore, the USB device knows which publisher it belongs to and how to find their administration server in order to check for available access and decryption keys.

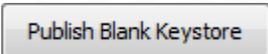
You might want to publish a blank keystore to a USB device if you want users to be able to use the USB device as an alternative to the Secure Viewer that has to be installed on individual computers.

Publishing the Viewer software and a blank keystore means that authorized users who have roaming profiles, for example, can download your protected documents from the Internet and (provided the relevant administration server has licenses for them) view them just as if they had installed the desktop Viewer.

This may also be convenient for use in situations where IT departments don't allow users Windows Admin rights to install any software, or have strict firewall policies in place that prevent registration of the desktop Viewer software.

This option may also be useful for mass production purposes, since USB devices can be initialized in large numbers and then be personalized ad-hoc at a later stage with documents and keys.

The  button is available when you first load Safeguard PDF Portable provided that no documents are selected in the GUI. If you have documents loaded in the GUI then you need to uncheck them for the

 button to become available.



NOTE: By publishing a blank keystore you WILL have to assign document/publication access on the administration system for the USB device since decryption keys will need to be obtained to allow access to the protected documents the user downloads in the future.

3.3.3 Producing larger volumes of secure USB devices

Because the keystore license has to be personalized to the absolute identity of the USB device itself, it is not possible to sub-contract the personalization of the keystore to a duplication company (although it is possible to have them put the collection of secure PDC files onto the USB device where there is a common list.)

When there is a requirement to produce more USB tokens than there are normal USB ports on the computer that is running the Writer application, it is possible to plug in one or more USB hub devices or daisy-chain from one hub to another). The USB 2.0 standard allows for multiple USB devices to be connected to a PC, but you cannot link directly or daisy-chain more than 127 devices onto a single port or exceed a total of 188 devices for the computer. There are also problems with overall bandwidth when trying to simultaneously address multiple USB devices and trying to exceed these numbers may prove counter-productive.

The Writer has been developed to identify the available USB devices that you can select, and when you give the Publish command it will step through the devices one at a time to upload the license files and any other files that you are adding to the device. This avoids problems with device and bandwidth conflicts, and may assist you in being able to remove USB devices as they finish being protected rather than having to wait until an entire batch has been processed (because you don't know which devices have finished being updated).

Chapter 4: Administering USB Devices

4.1.1 Managing USB devices

On your administration system a new Tab is available 'USB Devices'.

The screenshot displays the 'Safeguard PDF Security' administration interface. At the top, a blue header contains the title 'Safeguard PDF Security' and the user 'Logged In as: Jo'. Below the header is a navigation bar with tabs for 'Customers', 'USB Devices', 'Publications', 'Documents', 'Statistics', 'Settings', and 'News'. The 'USB Devices' tab is active. On the left, a sidebar contains 'Manage' and 'Export' options. The main content area is titled 'USB Devices' and includes a search filter, a 'Sort by' dropdown set to 'name', and a 'Show at least' dropdown set to '25'. Below these are links for 'Check', 'Uncheck', and 'Invert', and a 'With all checked' dropdown. A table lists USB devices, with one device shown: ID '0789115D2789', published on '07-18-2016', with a status of 'enabled' and 'valid from 07-18-2016'. The interface footer indicates 'Locklizard Administration System v4 (Build 170)'.

Diagram 8: USB Devices Tab

From here you can view the USB Devices you have populated, edit accounts, and assign document and publication access.

Clicking on the  button will display information relating to the USB device.

USB: AAG2KB0QWOQMHQ0T 

Name:

Email:

Company:

Notes:

Account Information

ID: 94

Status: **enabled**

Start Date: 

Valid until: 

never expires

Restrict IP: 

Manage Access

-  [Set Publication Access](#)
-  [Set Document Access](#)
-  [Change number of views](#)
-  [Change number of prints](#)

Event log

06-22-2016 14:49:29 - USB account created. USBID: AAG2KB0QWOQMHQ0T

Diagram 9: USB Details

4.1.1.1 *USB ID*

USB: AAG2KB0QWOQMHQ0T



This is shown at the top of the USB record. It displays the USB serial number. It is for information purposes only, and is used to identify a USB device. A user may require it to be able to identify their device if you need to update the documents they are authorized to use.

4.1.1.2 *Name, Email & Company*

By default the USB serial number is displayed in the Name field. You can change this information to that of a user name if you want to associate a particular user with a USB device. You may also want to populate the email and company fields with their details since this information will be picked up by the Viewer when using dynamic watermarking.

4.1.1.3 *Notes*

Here you can enter any information related to the USB device.

4.1.1.4 *Status*

This field shows if the account is enabled or suspended.

4.1.1.5 *Start Date*

Because users do not have to register USB devices, setting a start date has no meaning because it does not stop users viewing documents before this date has been reached. However it is used when documents have been protected to publications that have the 'obey start date' selected.

4.1.1.6 *Restrict IP*

This feature is only available in Safeguard Enterprise.

You may want to enter an IP address or address range here if you only want the USB device to be used at certain locations (i.e. for a corporate environment you can restrict use so that it can only be used in the office, or a library might restrict it to addresses in its domain).



NOTE: Documents **MUST** be set to check with the administration server (verify document access=each time the document is opened) for this to be enforced.

4.1.1.7 *Set Publication & Document Access*

If you have published a keystore that is not a blank one to the USB device then decryption keys are already available to the user and you do NOT have to assign access here. The document and publication access records will display the documents/publications the USB device has been granted access to automatically.

The only reason why you would need to assign access here is because you have published either a blank keystore, or users want the user to be able to view additional documents to those already published on the USB device.

4.1.1.8 *Change number of Views & Prints*

If you have published protected documents to the USB device with limited views/prints, then you can grant additional views/prints here.

4.1.1.9 *Batch Changes*

The following Batch changes available from the **Customers Tab** > **Batch** menu option also affect USB devices.

- Change customers validity
- Delete customer accounts
- Grant document access to all customers
- Grant publication access to all customers

If you therefore, for example, grant specific document access to all customers then all USB devices will be granted access too.

4.1.2 Exporting USB records

This facility is provided to allow you to extract information pertaining to your USB devices that are held on the administration database.

Go to the  **USB Devices** tab select the  **Export** menu item.

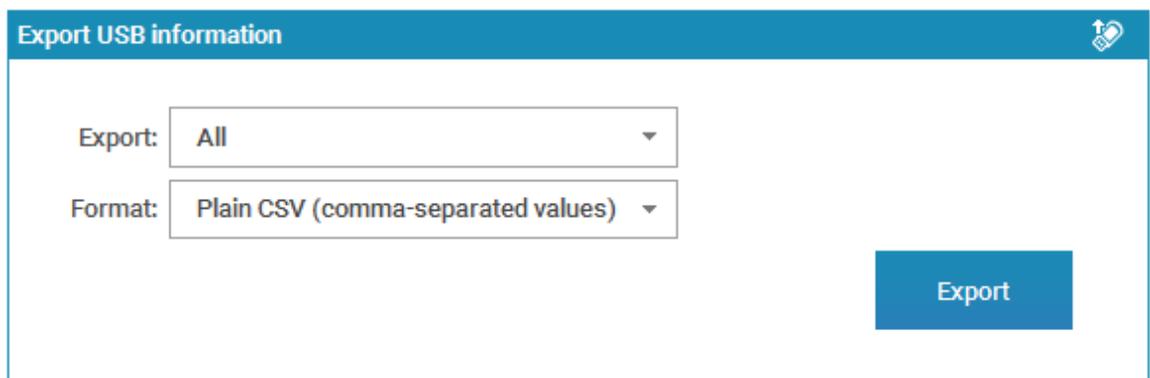


Diagram 10: Export USB records

4.1.2.1 *Export*

From this pull-down list box, choose the type of USB records you would like to export. The options are as follows:

- **All** – exports all USB records.
- **Suspended** – exports only suspended USB records.

4.1.2.2 *Format*

From this pull-down list box, choose the file format you would like your records to be exported to. The options are as follows:

- **Plain CSV** – exports information as a CSV file.
- **Zipped CSV** – exports information as a ZIP file with the contents in CSV format.

You may process the information provided in any suitable spreadsheet application.

Select the appropriate options corresponding to the data you want to export and then press the  button.

The following information is exported:

- USB ID
- Name
- Email
- Company
- Creation Date
- Status – enabled/suspended
- Expiry info
- Documents protected to the USB device
- Publication access



Chapter 5: Secure USB Viewer

This chapter describes the additional features available in the USB version of the Viewer.

5.1.1 Opening Secure Documents

5.1.1.1 Using the Autorun application

To view secure documents on a USB device, double-click on the file 'View Documents.exe'. This will open up a dialog with a list of the PDC documents available on the USB device.

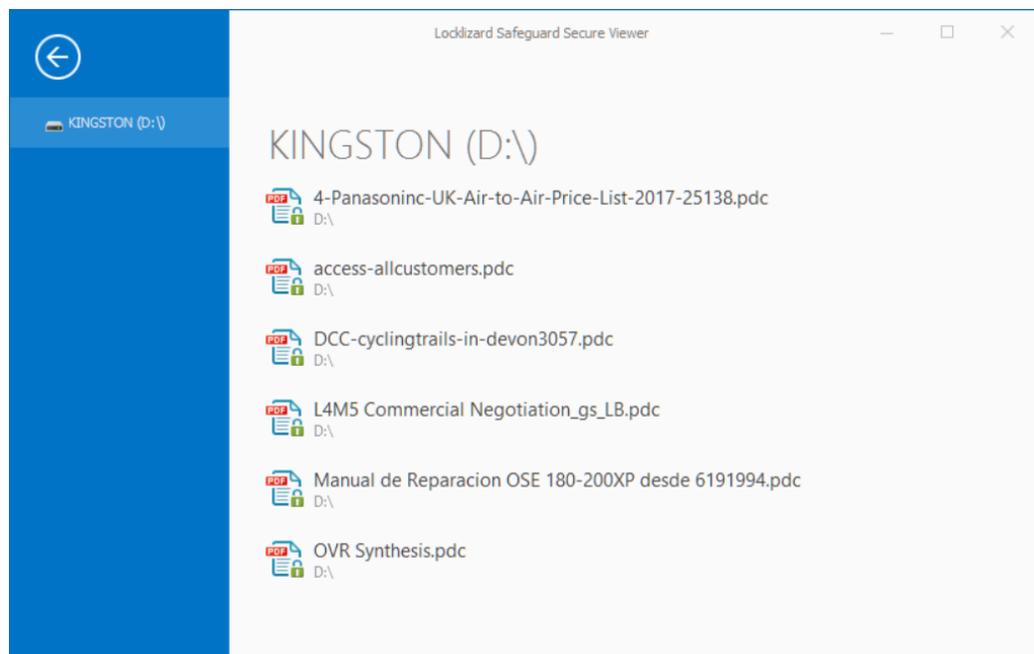


Diagram 11: Autorun interface (Safeguard v3 Viewer)

Click on a secure document to open it.



Diagram 12: Viewer with loaded document and USB Tab selected

5.1.1.2 *Associating the Viewer software with PDC files*

Alternatively, you can right-click on a PDC file and select 'Open With' > 'Choose Default Program', and then Browse for the Safeguard PDF Viewer application (pdcviewer64.exe) on your USB device. This can be found in the Viewer folder.

You will then be able to open subsequent secure documents by double-clicking on them.

5.1.2 **Keystore Password Protection**

Since USB devices are portable they can be easily lost or stolen, users have the option of setting a password to prevent misuse of the contents by others.

If a password has been set, then it has to be entered before a secure document can be opened.

5.1.2.1 Set Password

To set a password, open a PDC document on the USB device, and then select the 'Set USB Password' option from the USB Tab in the Viewer.

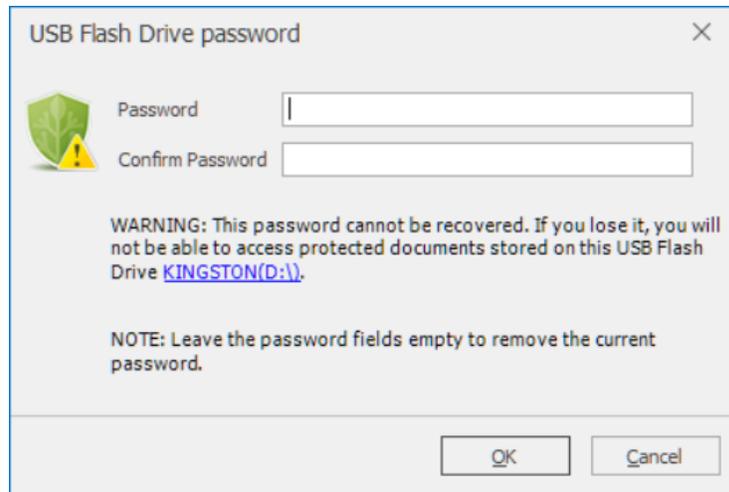


Diagram 13: Keystore Password dialog

 **IMPORTANT NOTE:** Make sure you make a note of the password as there is no way to recover it if it is lost/forgotten. You will not be able to open secure documents or remove your keystore if you forget it.

5.1.2.2 Change or Remove Password

To **change** the password, select the 'Set USB Password' option again.

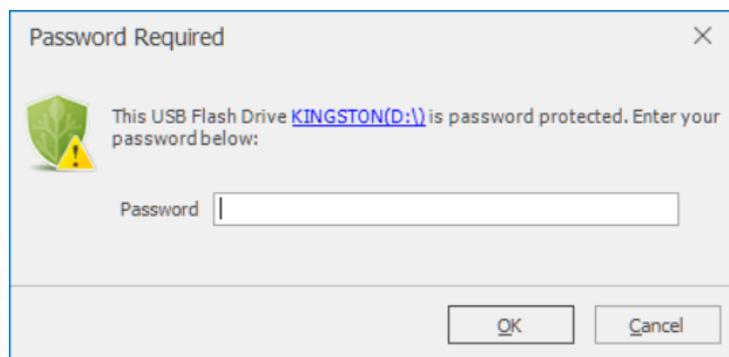


Diagram 14: Keystore Password entry

You will be asked for the current password, and if entered correctly, you can then enter your new password (the keystore password dialog as shown in diagram 13 will be displayed).

To **remove** the password, leave the passwords fields empty and press the OK button.

5.1.3 Remove Keystore

The Remove Keystore option is now available from the USB Tab.

It will create a blank keystore that remains registered to the publisher account that created it. After the keystore has been removed the Viewer will have to connect to the relevant administration server when opening secure documents for the first time in order to retrieve their decryption keys.



NOTE: If a keystore password has been set you will be asked to enter the password before the keystore can be removed.

5.1.4 USB ID

You may need from users the ID of the USB device they are using so you can assign additional access rights.

The actual USB ID is displayed when you hover over the Drive Letter (bottom right of the Viewer window).

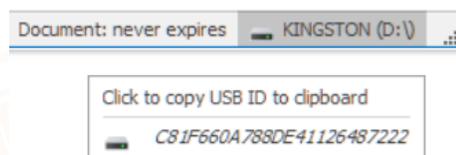


Diagram 15: USB ID

It is displayed when the Viewer on the USB is running regardless of whether a document has been opened or not.

To run the Viewer without opening a document (you may need to do this for example if a USB device was published with a blank keystore), navigate to the Viewer folder on your USB device and double-click on the application PDCViewer64.exe. Then use the back arrow on the left-hand side to return to the Viewer's main screen.

5.1.5 Program Updates

The Viewer update facility will update the Viewer software on the USB device. This only applies for USB devices that have the v3 Viewer installed.

If a USB device has a v2 Viewer installed on it and a user wants to upgrade it to v3 then they must first install the v3 Viewer on their computer. Then they must open a document on the USB device using the Viewer installed on their computer (the v3 Viewer). The Viewer will then ask them if they wish to upgrade.

User should close all Viewer sessions before doing the USB upgrade and make sure they don't interrupt or eject the drive while the upgrade process takes place – doing so may corrupt the USB contents.



This section covers frequently asked questions.

6.1.1 Do I have to re-protect my PDF files in order to use them with USB devices?

No. You select from existing PDC documents that you want users to be able to use from the USB device.

6.1.2 Do users have to download new documents to their USB devices or can they open them from their hard disk?

If the user is running the USB Viewer (they don't have the Viewer software installed on their computer) then they must copy the PDC documents to the USB device and open them from there.

6.1.3 Do users have to connect to a licensing server to register?

No. The USB device is automatically registered when you publish protected PDF documents (PDC files) to the device.

6.1.4 My documents connect to the Internet every time to verify access. How will they work with a USB Device?

They will work in exactly the same way as they did with the Secure Viewer installed on a computer. Even though the decryption keys may be present on the USB device, the Viewer will still check with the licensing server as instructed by the controls set in the document. If you decide to allow completely offline use of your documents on the USB device (never requiring an Internet connection) then you must make sure that the document controls that were set support this (no limited views, limited prints and so on).

6.1.5 How do dynamic watermarks work with USB devices?

The hardware ID of the USB device will be displayed unless you have edited the USB device account information on the administration system to include the user's name, company, and email address.

6.1.6 I have protected some documents to a USB device but I want users to download additional documents in the future. How will this work?

- If the documents are published as stand-alone documents (not to 'all customers' and 'outside of a publication') then you will need to go to your administration system and grant document access to that USB device. When the user opens those documents on their USB device, the USB Viewer will require a connection to your administration system in order to obtain the decryption keys for those documents.
- If the documents are published to 'all customers' then you won't have to grant additional access, but the USB Viewer must connect to your administration system the first time in order to obtain the decryption keys for those documents.
- If the documents are published to the same publication(s) as documents that are already on the USB device then you won't have to grant additional access, and the USB Viewer will not have to connect to the administration system, since it will already have the necessary decryption keys.
- If the documents are published to a different publication from documents that are already on the USB device then you will have to grant additional access, and the USB Viewer will have to connect to the administration system to obtain the decryption keys.

6.1.7 How can I make sure users only open secure documents from their work location?

Despite the fact that USB devices can be taken anywhere, you can make sure users only open secure documents from the locations that you choose. You do this by using the 'Restrict IP' option on the administration system (USB Devices > Details > Restrict IP field) and entering an IP address/range of IP addresses from where the USB device can be used. Be aware that this requires a connection to your administration server to verify the address range.

6.1.8 A user has forgotten their keystore password. What can I do?

There is no way to recover the keystore password so you will need to send them a new USB device containing your secure documents. You should allow for this possibility in agreements with users.

6.1.9 My USB devices were distributed by a third party. How do I identify a USB device with a user?

Ask the user to run the Viewer application. They can do this by navigating to the Viewer folder on your USB device and double-clicking on the application PDCViewer64.exe. The USB ID is displayed at the bottom right of the Viewer window when the mouse cursor is placed over the USB Drive Letter.

6.1.10 How can I protect content on USB devices whilst being sent by postal mail?

Since USB devices can be fully populated with secure documents and keystores that contain the decryption keys to open them, you may want to consider protecting the USB device whilst in transit.

You can do this in one of the following ways:

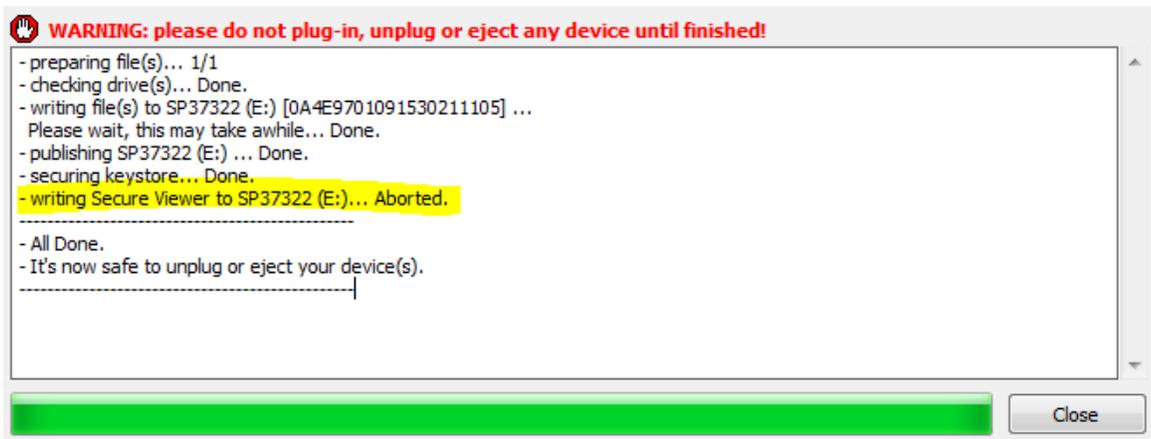
- Use a USB device that supports file encryption

- Password protect the keystore using the facility provide in the Secure Viewer software
- Ship a USB device with a populated keystore but without secure documents
- Ship a USB device with secure documents and a blank keystore

6.1.11 Error Message: Error loading component, cannot find one or more components

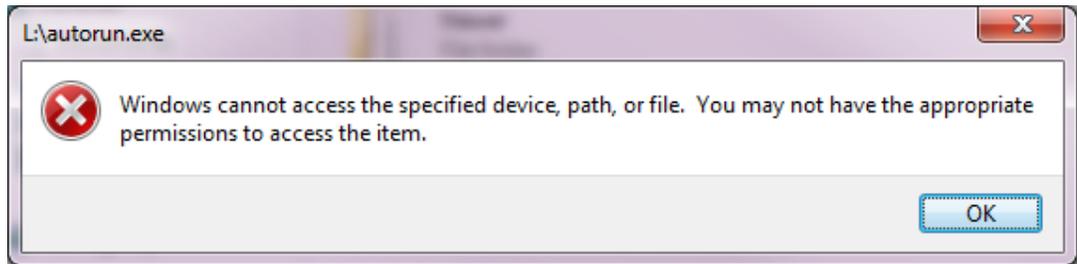
This message is displayed if you have installed Safeguard or Enterprise Writer straight over the top of a version that did not support Safeguard PDF Portable (Safeguard version 3.0.9 or below, and Enterprise 4.0.11 and below). You **must** completely de-install your existing Writer software (removing your Writer keystore first) and then you perform a fresh installation of the Writer software if you are not yet using a current version.

6.1.12 Why do I get an Aborted error when the Secure Viewer is being written to USB?



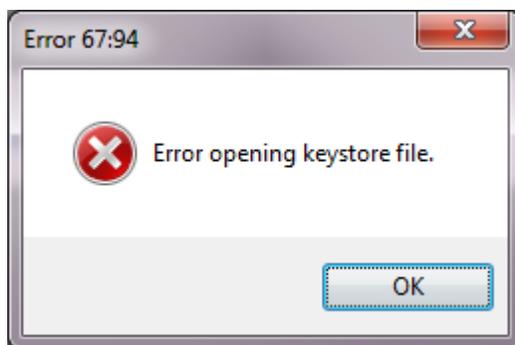
This is because either you have not installed the Secure Viewer software on your computer, or it is not in the default installation location. Safeguard PDF Portable expects to copy the Secure Viewer software from its default location on your computer to the USB device. If it is not present in that specific location then this step is aborted.

6.1.13 Error Message: Windows cannot access the specified device, path, or file, or file



This message is displayed if you do not have read or execute access set on the USB device. You need to ensure that you have execute, read, and write access in order to create and use protected documents.

6.1.14 Error Message: Error opening keystore file



This message is displayed if you do not have write access set on the USB device. You need to ensure that you have read, execute, and write access in order to create and use protected documents.

6.1.15 Error: The 'Protect to USB' application either does not load, or takes a long time to load

Remove any USB sticks you have plugged in. Load the application again and then plug the USB sticks back in.

6.1.16 Error: The 'Protect to USB' application hangs when protecting to USB devices

The most likely reason for this is that the device is in use or being held by another application. Check to see if Windows File Explorer is open with the device selected, and if it is, close it. Otherwise make sure that no other applications are connected to the USB device.

