KANGURU™

Secure. Anytime. Anywhere.

Evaluated Product

User Guide

Version 1.21

Notices and Information

Please be aware of the following points before using your Kanguru product

Kanguru Solutions will not be held responsible for any illegal use of this product nor any losses incurred while using this product. The user is solely responsible for the copyright laws, and is fully responsible for any illegal actions taken.

Customer Service

To obtain service or technical support for your system, please contact Kanguru Solutions Technical Support Department at 508-376-4245, or visit www.Kanguru.com for web support.

Legal notice

In no event shall Kanguru Solutions' liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. Kanguru Solutions offers no refunds for its products. Kanguru Solutions makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Kanguru Solutions reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

Export Law Compliance

Regardless of any disclosure made to Kanguru Solutions pertaining to the ultimate destination of the specific Kanguru product, you warrant that you will not export, directly or indirectly, any Kanguru product without first obtaining the approval of Kanguru Solutions and the appropriate export license from the Department of Commerce or other agency of the United States Government. Kanguru Solutions has a wide range of products and each product family has different license requirements relative to exports.

End User License Agreement

This legal document is an agreement between you, the end user ("Licensee"), and Kanguru Solutions, a division of Interactive Media Corporation ("Licensor").

By downloading or obtaining and using this software, you are consenting to be bound by the terms of this agreement, which includes the software license and software disclaimer of warranty.

This agreement constitutes the complete agreement between you and licensor. If you do not agree to the terms of this agreement, cease to use the product immediately and destroy any copies that you have made.

Software License

"The software" shall be taken to mean the software contained in this package, downloaded from Licensor's website, or included within a hardware device and any subsequent versions or upgrades received as a result of having purchased this package. "Licensee" shall be taken as the original purchaser of the software.

Licensee has the non-exclusive right to use the software only on a single computer. Licensee may not electronically transfer the program from one computer to another over any type of network. Licensee may not distribute copies of the software or the accompanying documentation to others either for a fee or without charge. Licensee may not modify or translate the program or documentation. Licensee may not disassemble the program or allow it to be disassembled into its constituent source code.

This software is licensed only to you, the Licensee. You may not permit non-Licensees to use or install it on computers or networks other than explicitly specified in this license without the prior written consent of Licensor.

This license does not entitle you to any future upgrades or updates of software or configuration files, although Licensor may decide to make such upgrades or configuration file updates available with or without an associated fee.

Licensee's use of the software indicates his/her acceptance of these terms and conditions. If Licensee does not agree to these conditions, then he or she must return any distribution media, documentation, and associated materials to the vendor from whom the software was purchased, and erase the software from any and all storage devices upon which it may have been installed or otherwise stored.

Disclaimer of Warranties

The software is provided on an "AS IS" basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose, and non-infringement. The entire risk as to the results and performance of the software is assumed by you, the Licensee. If the software is defective, you, and not Licensor or any distributor, agent or employee of Licensor assumes the entire cost of all necessary servicing, repair, or correction.

Limitations of Damages

In no event shall Licensor, or anyone else who has been involved in the creation, distribution, or delivery of this product be liable for any direct, indirect, special, punitive, exemplary, consequential or incidental damages (including but not limited to damages for loss of business profits, business interruption, loss of business information, and the like) arising out of the use or inability to use such product even if Licensor has been advised of the possibility of such damages. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Copyright Restrictions

This software and any accompanying materials are copyrighted. Unauthorized copying of this software or of any of the textual materials accompanying it is expressly forbidden.

You may not modify, adapt, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), or create derivative works based on the software.

Export Restrictions

You agree that you will not export the software to any country, person or entity subject to U.S. export restrictions.

Entire Agreement

This written End User License Agreement is the exclusive agreement between you and Licensor concerning the software and supersedes any and all prior oral or written agreements, negotiations or other dealings between us concerning the software. This License Agreement may be modified only by a writing signed by you and Licensor.

This agreement is subject to the laws and jurisdiction of the courts of the Commonwealth of Massachusetts, USA. If a court of competent jurisdiction invalidates one or more of the terms of this contract, the surviving terms continue in force.

This License Agreement is effective upon the earlier of your (1) use of the software; or (2) your manifesting assent to these terms as by clicking on the I Agree button shown when you downloaded or installed the software.

Table of Contents

1. Introduction

1.1 Purpose of this document

The Kanguru Defender Family of encrypted storage devices is designed to provide secure and reliable portable storage.

Because security requirements are dependent upon the applications and environment, it is not possible to simply certify that the devices are “secure”, a more precise definition is needed.

The Common Criteria (CC) provides a widely recognized methodology for security certification of products. A CC evaluation is fundamentally a two-step process, consisting of defining the “security target” which describes the features that are to be evaluated, and then testing and verifying that the product actually implements these features with a sufficient level of assurance.

This document is a security guide that explains how to set up the evaluated configuration, and provides information to administrators and ordinary users to ensure secure operation of the Kanguru Defender devices. It is intended to be self-contained in addressing the most important issues at a high level, and refers to other existing documentation where more details are needed.

The document addresses both administrators and users and the different tasks they are involved in.

Knowledge of the Common Criteria is not required for readers of this document.

1.2 How to use this document

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt). Note that this document avoids the terms “SHOULD” and “SHOULD NOT” that are defined in RFC 2119.

Requirements are either absolute (and marked with MUST and equivalent terms), or entirely optional (in the sense of not affecting required security functions) and marked with RECOMMENDED, MAY or OPTIONAL.

If you follow the requirements in this document when setting up and using the devices, your configuration will match the evaluated configuration. Certain configuration options are marked as OPTIONAL and you MAY modify them as needed, but you MUST NOT make other changes, because they will make the system fail to match the evaluated configuration.

Of course, you MUST always use common sense. This document is not a formal specification, and legitimate reasons can exist to modify the device setup in ways not described here if that is necessary for the system to fulfill its intended purpose. Specifically, applying security patches released by the Kanguru is strongly RECOMMENDED even though that will cause a deviation from the evaluated configuration.

In cases where the requirements and recommendations in this document conflict with those in other sources (such as the provided manuals), the information in this configuration guide has higher precedence. You MUST follow the steps described here to reach the evaluated configuration, even if other documentation describes different methods.

2. Requirements and Assumptions

2.1 What is a CC compliant system?

A system can be considered to be "CC compliant" if it matches an evaluated and certified configuration. This implies various requirements concerning hardware and software, as well as requirements concerning the operating environment, users, and the ongoing operating procedures.

Strictly speaking, an evaluation according to the CC represents the results of investigation of the security properties of the target system according to defined guidelines. It must not be considered as a guarantee for fitness for any specific purpose, but will provide help in deciding the suitability of the system considering how well the intended use fits the described capabilities. It is intended to provide a level of assurance about the security functions that have been examined by a neutral third party.

The software MUST match the evaluated configuration. In the case of the Defender Family, this also requires that the installed supporting software (UKLA and KRMC) are the same. The documentation (including this guide) will specify permitted variations, such as modifying certain configuration files and settings.

Note: KLA and UKLA are one and the same and are used interchangeably with each other in the document.

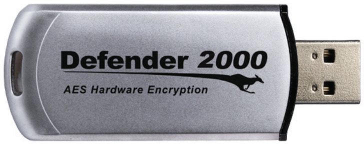
Stated requirements concerning the operating environment MUST be met. They are linked to the assumptions made in the Security Target.

Typical requirements are restrictions concerning permitted network connections (for the administrative access) and usage scenarios.

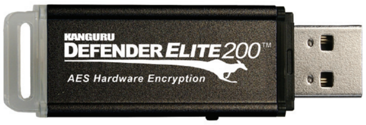
The operation of the system MUST be in agreement with defined organizational security policies, to ensure that actions by administrators and users do not undermine the system's security.

2.2 Identifying Your Defender Device

There are currently two Defender models that are certified for Common Criteria: 2000 and Elite200. You can visually identify which Defender model you own by checking the logo engraved on the device's casing.



Defender 2000



Defender Elite200

2.3 Hardware Requirements

The hardware MUST be one of the following devices. This entire document applies to all hardware systems unless explicitly noted.

- Kanguru Defender Elite200

Part number	Capacity	FW Version
KDFE200-4G	4GB	02.03.10 02.05.10
KDFE200-8G	8GB	
KDFE200-16G	16GB	
KDFE200-32G	32GB	
KDFE200-64G	64GB	
KDFE200-128G	128GB	

- Kanguru Defender 2000

Part number	Capacity	FW Version
KDF2000-4G	4GB	02.03.10 02.05.10
KDF2000-8G	8GB	
KDF2000-16G	16GB	
KDF2000-32G	32GB	
KDF2000-64G	64GB	
KDF2000-128G	128GB	

2.4 Software Requirements

The device client software MUST be one of the following applications. This entire document applies to all of the applications unless explicitly noted. The appropriate device specific Kanguru Defender Manager has to be used.

- Kanguru Defender Manager Elite200:
  - KDME200 v 2.0.0.0 - 2
  - KDME200 v 2.0.0.0 - 3
  - KDME200 v 2.0.0.0 - 6
- Kanguru Defender Manager 2000:
  - KDM2000 v 1.2.1.8 - 2
  - KDM2000 v 1.2.1.8 - 3
  - KDM2000 v 1.2.1.8 - 6
- Universal Kanguru Local Administrator: *Version Release 3.2.0.3*
- Kanguru Remote Management Console: *Version 5.0.2.6*

Important! Your Defender security device MUST be running the Kanguru Defender Manager software version listed above in order to be considered CC compliant. It is the user's responsibility to ensure that their hardware is in compliance. For instructions on determining what version of Kanguru Defender Manager your device is running, please refer to section 4.4 *KDM* on page 18.

2.5 Requirements for the system's environment

The security target covers devices that use Linux, MacOS and Windows hosts for access via the appropriate Kanguru Defender manager (KDM).

It is assumed that the value of the stored assets merits moderately intensive penetration or masquerading attacks. It is also assumed that physical controls in place would alert the system authorities to the physical presence of attackers within the controlled space.

You MUST use the devices only on trustworthy hosts that can be relied on to not have any malware installed.

The Kanguru Remote Management Console MUST be installed on a Windows 2008 System with MS SQL Server 2005, MS SQL Server 2008 or MS SQL Express and IIS already installed and the latest security patches applied.

The Kanguru Remote Management Console MUST be installed on a physically protected system that is only used for KRMC.

The Kanguru Central Server MUST NOT be used in the evaluated configuration.

2.6 Requirements for administrators

When using the devices in an Enterprise configuration, there MUST be one or more competent individuals who are assigned to manage the devices. These individuals will have the ability to initialize and reset devices, reset and change user passwords as well as configure failed authentication handling.

The system administrative personnel MUST NOT be careless, willfully negligent, or hostile, and MUST follow and abide by the instructions provided by the administrator documentation.

Every person that has the ability to perform administrative actions via UKLA and KRMC has control over security properties of the devices and could, either by accident or deliberately, undermine security features of the system. This Configuration Guide provides the basic guidance on how to set up and operate the system securely, but is not intended to be the sole information required for a system administrator to learn how to operate the devices securely.

It is assumed, within this Configuration Guide, that administrators who use this guide have a good understanding and knowledge of operating security principles in general and of the Defender configuration in particular. We strongly advise that any organization that wants to operate the system in the evaluated configuration nevertheless have their administrators trained in security principles.

Every organization MUST trust their system administrators not to deliberately undermine the security of the devices.

This Configuration Guide provides the additional information a system administrator MUST obey when installing, configuring and operating the devices in compliance with the requirements defined in the Security Target for the Common Criteria evaluation.

2.7 Requirements for users

Users MUST inspect the device and packaging before use to verify that it has not been tampered with. The casing and any sealing (of the original packaging) MUST be intact without any marks. If the casing or seal is broken or has been tampered with, users MUST refuse delivery of the package.

Users MUST ensure that the authentication attribute can not be obtained by spying or shoulder surfing.

Users MUST ensure that the system that they use to access the devices are secure and do not contain any software that tries to access the devices in an unauthorized fashion.

Users MUST protect the host computer while absent (e.g. via a screen locker) while a device is connected or disconnect the device.

Users MUST check that the firmware version on the device is the correct CC certified version. For instructions on verifying the device’s firmware version and a comprehensive list of CC certified version, please refer to Chapter 5. *Common Criteria Certified Versions* on page 25.

2.8 Requirements for connectivity

When using KRMC, you MUST ensure that all network connections used for the communication with the KRMC are under the same management domain as the TOE and protected against tampering, tapping and other modifications.

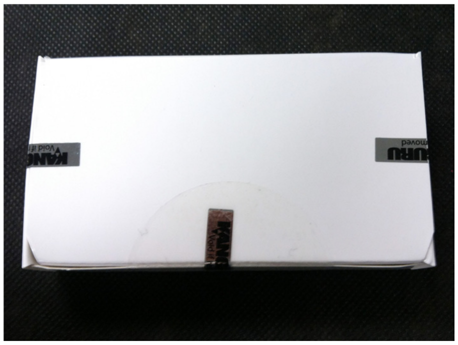
2.9 Excluded functionality

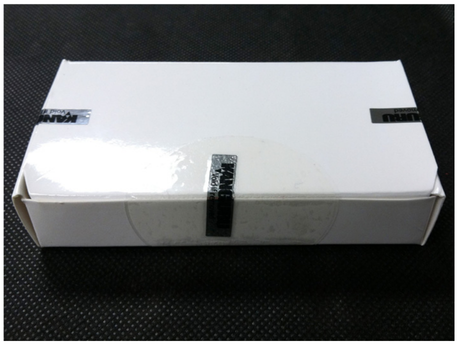
The Kanguru Defender devices support more functionality than what is covered by the evaluation, namely antivirus, the virtualization component, the write protect switch and KRMC cloud.

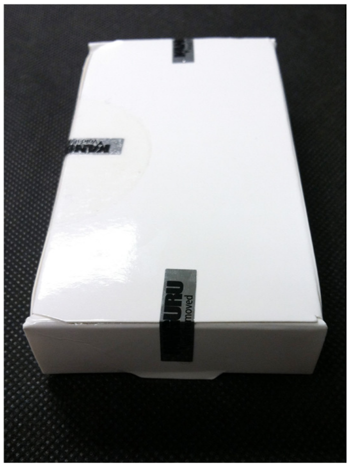
Use of these features have not been evaluated as part of the CC Configuration.

2.10 Device reception

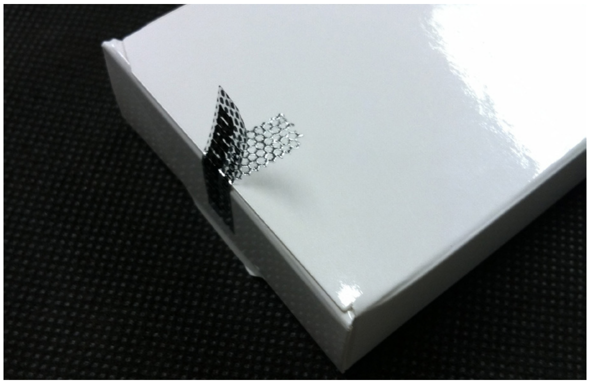
The open edges of the Kanguru Defender's packaging are secured by three tamper evident seals which cannot be removed without leaving behind visual indication that the seals have been removed. When initially receiving the device, the administrator or user MUST ensure that the device arrives in a package with seals that are not broken.







Seals that have been tampered with will leave behind a distinct pattern of dots. If any of the seals are broken or have been tampered with, the customer MUST refuse delivery of the package.



3. Documentation

The delivery of the Guidance Documents will be secured through a secure site (Kanguru.com). The document will be available as a download with a SHA256 hash available to confirm that the download is authentic and uncompromised.

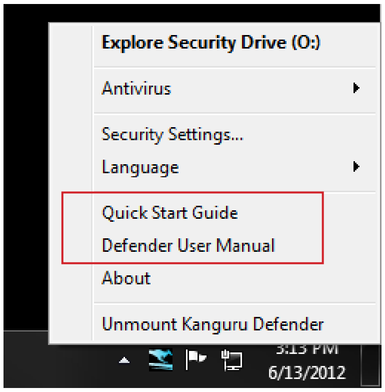
Important! The user MUST check the authenticity of the documentation downloaded to ensure that the files have not been corrupted or tampered with. The user can use file hashing to verify that the file they downloaded is genuine. For instructions and details on verifying the file hash, please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.

This document (Common Criteria Document) takes precedence over all user manuals.

- Defender Elite200: https://kanguru.zendesk.com/entries/89657676
- Defender 2000: https://kanguru.zendesk.com/entries/89657676
- UKLA: https://kanguru.zendesk.com/entries/90082416
- KRMC: https://kanguru.zendesk.com/entries/88927863

In addition, these documents are also available for download through the software applications.

- To download digital copies of Kanguru Defender 2000 and Elite200 documentation, right-click on the KDM icon located in the task bar. The Defender menu appears.
    - ○ Click on **Quick Start Guide** to download a digital copy of the Defender's Quick Start Guide
    - ○ Click on **Defender User Manual** to download a digital copy of the Defender's User Manual



- To download a digital copy of the KRMC documentation, login to KRMC and then click on **Support → Manuals → Documentation**

ECG delivery to customers
Customers can download latest evaluated guide from Kanguru support site at:
https://kanguru.zendesk.com/entries/88351486-Evaluated-Product-Guide

CC Certified User manuals can be downloaded from:

- https://kanguru.zendesk.com/entries/89657676-Evaluated-User-Guides-for-Devices
- https://kanguru.zendesk.com/entries/90082416-Evaluated-User-Guide-for-UKLA
- https://kanguru.zendesk.com/entries/88927863-Evaluated-User-Documents-KRMC

Access to the UKLA and KRMC User Manuals is granted to UKLA and KRMC administrators when their order is processed.

4. Software Installation

The evaluation covers a fresh installation of the management software and the initial configuration of the devices listed in section 2.3 *Hardware Requirements* on page 9.

4.1 Obtaining copies of UKLA and KRMC

Both UKLA and KRMC are only available after they have been purchased. There are two ways that you can obtain the UKLA and KRMC installer package:

- Physically provided on a CD
- A digital copy can be downloaded from the Kanguru Solutions' support site

Unless you specify otherwise when placing your UKLA or KRMC order, a UKLA and/or KRMC installation disc will be shipped to you.

Verifying the installation CD

Installation CD's are packaged at secure Kanguru facilities and shipped via industry standard supply chain organizations (UPS, FedEx, etc). All shipped CD's are sealed when packaged and protected with a tamper evident seal. If the seal is broken or has been tampered with, customers MUST refuse delivery of the package.

Digital Download

To obtain access to digitally download the UKLA/KRMC installation package, please send an e-mail request to krmc_support@kanguru.com with your order information. Once your order information has been confirmed, you will receive an e-mail notifying you that access to the UKLA/KRMC installer download has been granted.

These files are only accessible to registered users who have been granted access to the Kanguru UKLA and KRMC web portal:

- UKLA download: https://kanguru.zendesk.com/entries/74698328
- KRMC download: https://kanguru.zendesk.com/entries/74056153

Important! The user MUST check the authenticity of the downloaded installers to ensure that the files have not been corrupted or tampered with. The user can use file hashing to verify that the file they downloaded is genuine. For instructions and details on verifying the file hash, please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.

4.2 UKLA

UKLA can be installed anywhere on your Windows system. You MUST place it in a directory that is writable by the user ID working with it, as it writes a settings file into this directory.

Please refer to the “UKLA User Manual v3.2.1.pdf” before the first use of the software.

When running UKLA for the first time you will be prompted to set up an administrator password. This password MUST conform to the password guidance given in the Password selection policy.

Update UKLA
Updates to UKLA are released by Kanguru Solutions regularly. The Update UKLA section allows you to check for any available updates to your Universal KLA software version. Your computer will need to have access to the internet in order to check for newer versions of UKLA.

Click on the **Check for software updates** button**.** UKLA will connect to the Kanguru Central Server and check whether there are any updates available. If an update is available, you MAY follow the on-screen instructions to update your version of UKLA.

WARNING! You will receive a warning message if your UKLA version is Common Criteria certified. If you update UKLA from a Common Criteria certified version to a newer version, the software application will no longer be Common Criteria certified.

4.3 KRMC

Please refer to “KRMC - Enterprise Edition - Install Guide v5.pdf” for instructions on installing KRMC and the prerequisite software (MS SQL and IIS on Windows Server 2008).

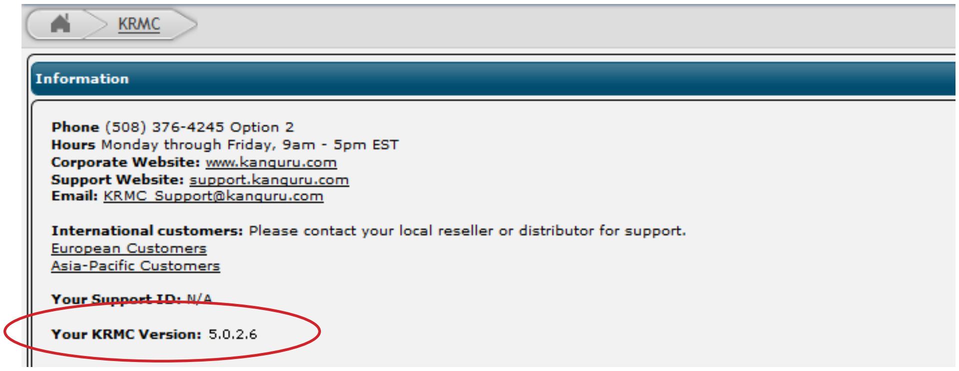
When setting up the MS SQL Server, the passwords used for the database MUST conform to the password guidance given in the Password selection policy.

The passwords used for the CA that is installed with KRMC MUST conform to the password guidance given in the Password selection policy.

The Device Control module is optional and is not part of the CC evaluation. You MUST NOT enable Device Control functionality.

When running KRMC for the first time you MUST change the supplied default password for the administrator. The new password MUST conform to the password guidance given in the Password selection policy.

To view the version of KRMC currently running, go to the Support section in your KRMC console. The Support page provides you with information regarding your KRMC version, server time zone, system configuration, and information for contacting Kanguru’s Technical Support staff.



Phone (508) 376-4245 Option 2
Hours Monday through Friday, 9am - 5pm EST
Corporate Website: www.kanguru.com
Support Website: support.kanguru.com
Email: KRMC_Support@kanguru.com

International customers: Please contact your local reseller or distributor for support.
European Customers
Asia-Pacific Customers

Your Support ID: N/A

Your KRMC Version: 5.0.2.6

Important! If you have been using a non-CC compliant version of KRMC and want to migrate to a CC compliant version, you MUST make a fresh install of the CC compliant KRMC version. For a KRMC Enterprise migration to a CC certified version, the administrator of the enterprise environment will need to follow these steps:

1. Uninstall the current KRMC installation by following the steps below:
   a. Remove the Kanguru Remote Management Console from **Windows Control Panel → Add/Remove Programs**
   b. Remove KRMC from the IIS sites list
   c. Remove the KRMC folder from within **inetpub → wwwroot** folder path
2. Restart the server where KRMC was installed.
3. Download the CC Certified KRMC installer version from the Kanguru Support site.
4. Install the CC Certified version of the KRMC server downloaded from the Kanguru site.

4.4 KDM

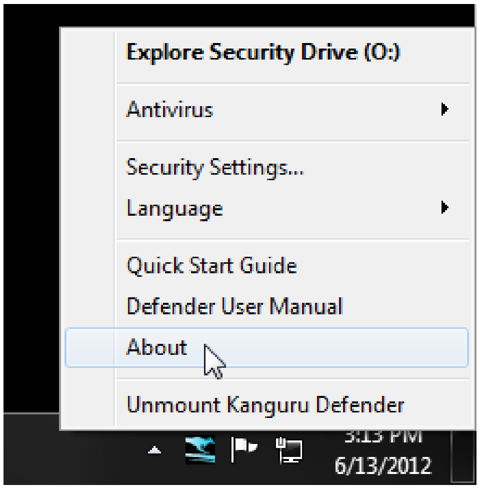
The Defender 2000 and Elite200 flash devices come pre-loaded with firmware and KDM client software. For all drives, the delivery to the customer is carried out by a commercial delivery service, such as UPS, USPS, FedEx, etc.

The Defender Device contains two partitions: a CD-ROM partition and a secure, encrypted partition. Kanguru Defender Manager (KDM) is the client program pre loaded on the Defender Device's CD-ROM partition. The user needs to login to KDM in order to access the secure, encrypted partition. KDM comes pre-installed on your Defender Device. No installation on your PC is necessary.

4.4.1 Verifying the KDM Software Version

Users can open the **version.ini** file in CD-ROM partition to verify the software version on their drive. The CC certified software versions are mentioned in this doc (see section 2.4 *Software Requirements* on page 10) as well as in the device's user manual.

Users are able to view the version of the KDM client application currently running on their drive by right-clicking on the KDM icon located in the task bar and then selecting **About**.



Important! Your Defender security device MUST be running a CC certified version of the Kanguru Defender Manager software to be considered CC compliant (i.e. *KDME200 v2.0.0.0* or *KDM2000 v1.2.1.8).* Your Defender device MAY have come pre-loaded with a non-CC certified version of KDM. If your Defender device is not running a CC certified version of KDM, please see section 4.4.3 *Updating Your Defender Device* on page 21 for information on updating your Defender's KDM software version to a CC certified version.

4.4.2 Verifying the KDM Client Edition

Users can open the **version.ini** file in CD-ROM partition to verify whether their device is running a Cloud edition, Enterprise edition or No-Comms edition client.

Open the **version.ini** file in a text editor and check the line for “Product Version” and check whether the product version number ends in - 2, - 3 or - 6 suffix.

Version suffix	Edition	Description
-2	Cloud edition	The standard Defender model.
-3	Enterprise edition	Enterprise edition devices have been configured to be capable of communicating with KRMC Enterprise.
-6	No-Comms edition	The No-Comms version is identical to the Cloud version but with all communication functionality disabled.

Some other general differences are identified below:

In KDM Cloud:

- Anti-Virus (AV) definitions are downloaded from Kanguru server. The list with the most current definitions is received from the Kanguru Central Server (KCS). **Important!** KDM Cloud edition users MUST disable anti-virus functionality on their device.
- Cannot be managed by KRMC Enterprise

In KDM Enterprise:

- AV definitions are downloaded from a KRMC enterprise server. **Important!** KDM Enterprise edition administrators MUST disable anti-virus functionality for their managed devices.
- Devices MUST be provisioned using UKLA - setting device properties and exporting them to a .krm file that is added in KRMC Enterprise.
- “Enterprise Edition” appears on the splash screen

In KDM No-Comms:

- There is no AV functionality.
- There is no communication to any network or internet server.
- All drive communications, including live updates for the KDM client software for the drive, are disabled.
- The drive operates in a completely offline mode, and cannot be managed by KRMC.

Verifying the files loaded to your Defender device

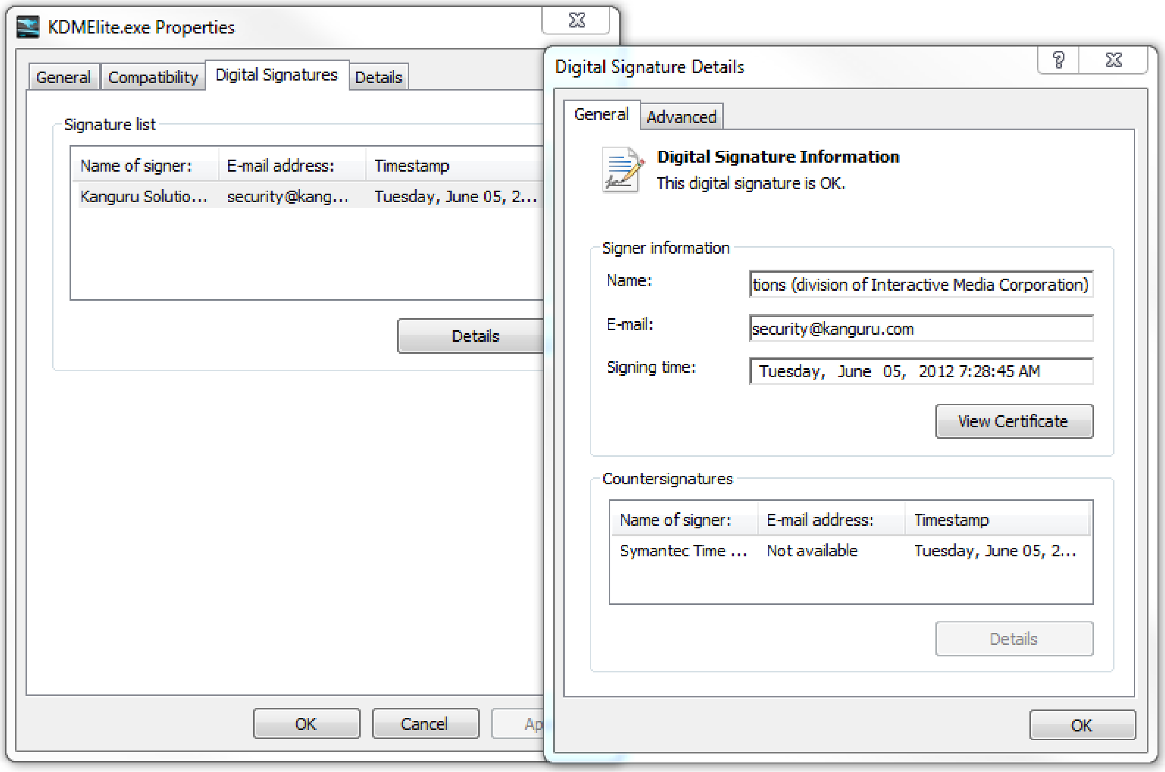
The user MUST check the authenticity of the client software on their Defender drive to ensure that the device has not been corrupted or tampered with. The user can use file hashing to verify that the files contained on their devices are genuine. For instructions and details on verifying the file hashes, please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.

Verifying the client application certificate information

Windows users can check that the digital certificate for the KDM client application is signed by Kanguru Solutions, in order to guarantee its authenticity. This feature is only available through Windows and is not available for Mac OSX or Linux users.

To verify the certificate information:

1. Open the Defender's CD-Rom partition in Windows Explorer.
2. Right click on the KDMxxxx.exe client application file and select **Properties** from the menu.
3. Click on the **Digital Signature** tab.
4. In the signature list, select Kanguru Solutions and then click on the **Details** button.
5. Check that the digital signature is OK and that "Kanguru Solutions (division of Interactive Media Corporation)" is listed as the name under Signer Information.



Name of signer:	E-mail address:	Timestamp
Kanguru Solutio…	security@kang…	Tuesday, June 05, 2…

Digital Signature Information
This digital signature is OK.

Name: tions (division of Interactive Media Corporation)
E-mail: security@kanguru.com
Signing time: Tuesday, June 05, 2012 7:28:45 AM

Name of signer:	E-mail address:	Timestamp
Symantec Time …	Not available	Tuesday, June 05, 2…

4.4.3 Updating Your Defender Device

For the purposes of this section, the word "device" is taken to refer to either the Kanguru Defender 2000 or Kanguru Defender Elite200 secure encrypted drives. The instructions below apply to both secure devices.

Updates for your Defender device's client application are released from time to time and you MAY receive a Defender device running a CC non-compliant version of the client software. You MUST check whether your Defender device is a no-comms edition device, cloud edition device or managed by Kanguru Remote Management Console Enterprise (KRMC Enterprise), as the update process is different for enterprise edition, no-comms and cloud/standard edition drives. Please refer to section 4.4.1 *Verifying the KDM Software Version* on page 18 for information about verifying which device edition your Defender is.

If a user has purchased drives with a certain build type (E.g.: Cloud) but wishes to migrate to another build type, he MAY do so using the CC downgraders designed for the drive type ordered, but they MUST conform to the upgrade path options identified below.

Upgrade paths possible:

- From Cloud client – To Cloud or Enterprise client
- From Enterprise client - To Enterprise client
- From No-Comms client – To No-Comms client

It is the sole responsibility of the administrator to verify and confirm that the Defender devices are running a common criteria certified version of the client application.

Verifying the CC Certified Downgrader application

The user MUST check the authenticity of the CC certified downgrader application to ensure that the file has not been corrupted or tampered with. The user can use file hashing to verify that the file is genuine. For details on verifying the file hash, please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.

Verifying the client updater certificate information

Windows users MAY check that the digital certificate for the KDM updaters are signed by Kanguru Solutions to guarantee its authenticity. This feature is only available through Windows and is not available for Mac OSX or Linux users.

To verify the certificate information:

1. Right click on the client updater file and select **Properties** from the menu.
2. Click on the **Digital Signature** tab.
3. In the signature list, select Kanguru Solutions and then click on the **Details** button.
4. Check that the digital signature is OK and that "Kanguru Solutions (division of Interactive Media Corporation)" is listed as the name under Signer Information.

4.4.3.1 Updating Cloud/Standard Edition Devices

To prevent you from accidentally updating your device to a non-Common Criteria certified client version, the client application's auto-update feature has been disabled on Common Criteria certified Devices. Device updates cannot be downloaded through the client.

Cloud/Standard edition Defender users MAY manually search and download available client updaters from the Kanguru Support site. Defender client updaters are found under the 'USB Client Software Updates' forum in the 'Software Downloads and Updaters' section (support.kanguru.com). Client updaters for CC certified versions are prominently labeled as such.

- Kanguru Defender Elite200 Cloud/Standard Edition link on support site:
  https://kanguru.zendesk.com/entries/63158227
- Kanguru Defender 2000 Cloud/Standard Edition link on support site:
  https://kanguru.zendesk.com/entries/63713336

Migrating from non-CC certified device to CC certified version

If you are migrating a non-CC certified device to a CC certified version, then it is RECOMMENDED to backup all user data or applicable settings before attempting these instructions, as doing so may lead to the drive being reset and all stored user data being erased permanently.

1. Check the device for any evidence of physical damage that could hint at the device being compromised.
2. Reset the device using the **Reset button** on the Kanguru Defender Manager login screen.
3. Download the CC certified downgrader application for your device from the Kanguru support site.
4. Execute the downgrader application. This will migrate the current software version on the user device to the CC certified version.
5. After the update is complete, you MUST verify that the files on the updated CD-ROM partition are authentic. Please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.

4.4.3.2 Updating KRMC Enterprise Edition Devices

Enterprise edition Defender devices are managed by the Kanguru Remote Management Console (KRMC). Updaters for enterprise edition Defender devices are available for download from the Kanguru Support site. The KRMC system administrator is granted access to the enterprise edition downloads when their KRMC order is processed.

KRMC Enterprise administrators can manually download the available client updaters from the Kanguru Support site. Only KRMC administrators are given access to download the enterprise edition updaters. Client updaters for CC certified versions are prominently labeled as such. Once you have downloaded your enterprise edition updater, create an 'Upgrade Client Application' action in KRMC to deploy the update to all of your managed drives remotely.

- Kanguru Defender Elite200 Enterprise Edition Updater link on support site: https://kanguru.zendesk.com/entries/75199226

- Kanguru Defender 2000 Enterprise Edition Updater link on support site: https://kanguru.zendesk.com/entries/74685198

Migrating from non-CC certified device to CC certified version

If you are migrating a non-CC certified device to a CC certified version then the administrator will need to have the drives brought in and then follow the below steps. It is RECOMMENDED to backup all user data or applicable settings before attempting these instructions, as doing so may lead to the drive being reset and all stored user data being erased permanently.

1. Check each device for any evidence of physical damage that could hint at the device being compromised.
2. Reset the device using the Universal Kanguru Local Administrator (UKLA) provided by Kanguru Solutions.
3. Download the CC certified downgrader application for the devices from the Kanguru support site
4. Execute the downgrader application. This will migrate the current software version on the user device to the CC certified version.
5. After the update is complete, you MUST verify that the files on the updated CD-ROM partition are authentic. Please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.
6. Re-provision the device for the enterprise specific settings using UKLA.

4.4.3.3 Updating No-Comms Edition Devices

To prevent you from accidentally updating your device to a non-Common Criteria certified client version, the client application's auto-update feature has been disabled on Common Criteria certified Devices. Device updates cannot be downloaded through the client.

No-Comms device users can also manually search and download available client updaters from the Kanguru Support site. Defender client updaters can be found under the 'USB Client Software Updates' forum in the 'Software Downloads and Updaters' section (support.kanguru.com). Client updaters for CC certified versions are prominently labeled as such.

- Kanguru Defender Elite200 No-Comms Edition Updater link on support site:
  https://kanguru.zendesk.com/entries/95109883

- Kanguru Defender 2000 No-Comms Edition Updater link on support site:
  https://kanguru.zendesk.com/entries/96263006

Migrating from non-CC certified device to CC certified version

If you are migrating a non-CC certified device to a CC certified version then the administrator MUST have the drives brought in and then follow the below steps. It is RECOMMENDED to backup all user data or applicable settings before attempting these instructions, as doing so may lead to the drive being reset and all stored user data being erased permanently.

1. Check the device for any evidence of physical damage that could hint at the device being compromised.
2. Reset the device using the **Reset button** on the Kanguru Defender Manager login screen.
3. Download the CC certified downgrader application for your device from the Kanguru support site.
4. Execute the downgrader application. This will migrate the current software version on the user device to the CC certified version.
5. After the update is complete, you MUST verify that the files on the updated CD-ROM partition are authentic. Please refer to Chapter 11. *Verifying Your Files Using SHA256 Checksum* on page 29.

5. Common Criteria Certified Versions

Defender Elite200's with the following specifications have been certified by Common Criteria:

- Client software version : **2.0.0.0-2**, **2.0.0.0-3**, **2.0.0.0-6**
- Firmware version : **02.03.10, 02.05.10**

Defender 2000's with the following specifications have been certified by Common Criteria:

- Client software version : **1.2.1.8-2**, **1.2.1.8-3**, **1.2.1.8-6**
- Firmware version : **02.03.10, 02.05.10**

The following version of UKLA has been certified by Common Criteria:

- Universal Kanguru Local Administrator version : **3.2.0.3**

The following version of KRMC has been certified by Common Criteria:

- Kanguru Remote Management Console version : **5.0.2.6**

5.1 Firmware verification Process

Kanguru provides a tool called FW tool. Users MAY plug in their device and run the tool to get the firmware versions on their devices.

The FW tool can downloaded from Kanguru's support site at the following location: https://kanguru.zendesk.com/entries/22974561-firmware-display-tool

5.2 Client Software Verification Process

Users MAY check the **version.ini** file in CD-Drive partition to check the client software version for their device. The CC certified software versions are mentioned in this document as well as in the Device User Manual.

The **version.ini** file can be used to identify whether your device is a Cloud edition, Enterprise edition or No-Comms edition device. Open the **version.ini** file in a text editor and check the line for "Product Version". Note whether the product version number ends in - 2, - 3 or - 6

- - 2 is listed for Cloud edition devices
- - 3 is listed for Enterprise edition devices
- - 6 is listed for No-Comms edition device

Users are also able to view the version of the KDM client application currently running on their device after logging in by right-clicking on the KDM icon located in the task bar and then selecting **About**.

Important! It is the sole responsibility of the administrator to verify and confirm that the Defender devices are running a common criteria certified version of the client application. Your Defender device may not have come pre-loaded with a CC certified version of KDM. If your Defender device is not running a CC certified version of KDM, please see section 4.4.3 *Updating Your Defender Device* on page 21 for information on updating your Defender's KDM software version to a CC certified version.

6. Device Self Test

All devices feature an LED that indicates the state of the device as follows:

- After the device has been powered on via USB the LED blinks at about three blinks per second. This frequency is also kept during and after the initial self test (Power On Self Test or POST), after boot until the CD-ROM partition mounts, and then the LED is turned off.

- If the POST fails, then the LED blinks at a much higher frequency (16 blinks/s) and the USB data pins (D+/D-) between host computer and the device are disconnected. The device cannot be accessed via USB in this case.

- In a normal usage case when accessing the device, the LED blinks at 3 blinks/s. After 2.56 seconds without the device being accessed the LED turns OFF. When the device is not accessed or it is in USB suspend state, the LED is off.

7. Standalone Device Setup

A standalone device is not managed by UKLA or KRMC. All setup responsibility solely lies with the user. The use of the device MUST follow the guidance given in Chapter 2. *Requirements and Assumptions* on page 8.

Please refer to the KDM manual appropriate for your model of Defender device (KDME200 or KDM2000) for handling instructions.

When configuring a device for standalone use, KRMC Cloud functionality MUST be disabled and remain disabled.

Passwords MUST be selected according to the Password selection policy documented later in this document.

8. Managed Devices

Organizations can manage devices via UKLA and KRMC depending on the scope of the deployment and their security policies. UKLA is used for local, standalone device management as well as for priming devices for use with KRMC. The KRMC is used to manage large numbers of devices via the network.

When KRMC is used, all device actions are queued at the KRMC and polled by the KDM software and relayed to the devices when the devices are connected to their hosts running KDM.

When using UKLA or KRMC to mange devices, password rules according to Password selection policy MUST be set for the devices.

9. Password Selection Recommendation

The following password policy MUST be enabled for all parts of the TOE where possible (not all parts or prerequisite software allow the specification of special characters in passwords).

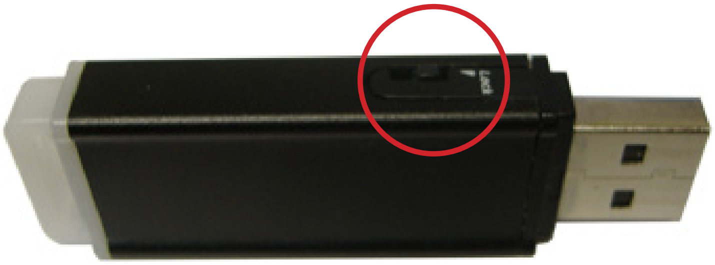
Passwords MUST be at least 12 characters long, containing at least one of each: uppercase character, lowercase character, number and special character.

It is RECOMMENDED that the life time of a password is no more than 6 months and that passwords not be re-used for at least six rounds.

The device MUST be disabled or erased after 7 or fewer consecutive unsuccessful events. **Note:** When using UKLA or KRMC, the default value consecutive unsuccessful attempts is set to 6 and MUST be adjusted.

10. Defender Elite200 Write Protect Switch

The Kanguru Defender Elite200 device features a physical write protect switch. When set in the locked position, the write protect switch will prevent any data from being written to the device.



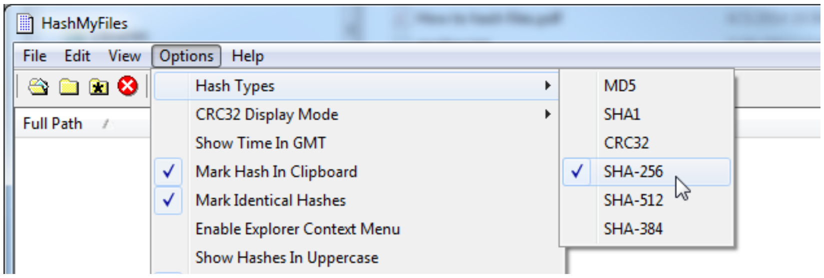
The Defender Elite200's write protect switch was not considered for Common Criteria evaluation. For more information regarding the physical write protect switch, please refer to the Defender Elite200 User Manual.

11. Verifying Your Files Using SHA256 Checksum

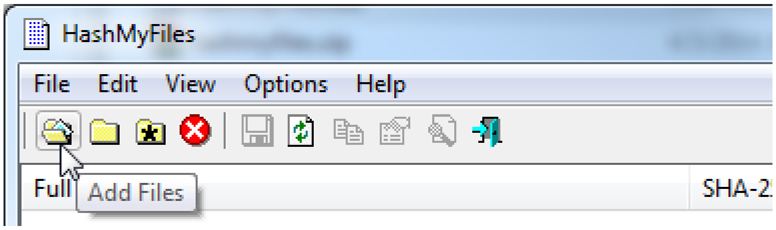
To verify the integrity of the KDM updater that you downloaded, please use the *HashMyFiles* SHA256 Checksum tool. *HashMyFiles* is a widely available Freeware application for Windows that can generate a 64-character checksum which can be verified against the checksum list published by Kanguru Solutions. This ensures that any files that you receive or that came loaded on your devices weren't altered in any way.

To view and verify your download's checksum:

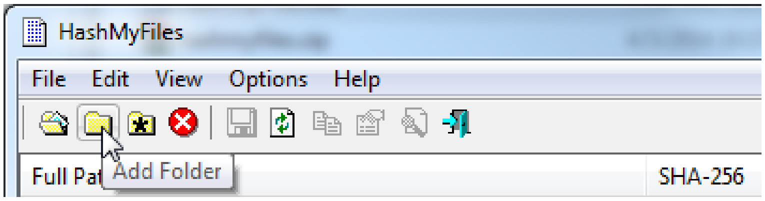
1. Download the *HashMyFiles* tool from the internet. A copy of the Freeware program is hosted on Kanguru Solutions' support site, or it can be downloaded directly from the publisher's website: http://www.nirsoft.net/utils/hash_my_files.html
2. Save *HashMyFiles* on your computer and extract the files to your local hard drive.
3. Double click on **HashMyFiles.exe** to run the application.
4. Go to the **Options menu** → **Hash Types** and make sure that only 'SHA-256' is selected.



5. Add the file(s) to the *HashMyFiles* console.
   ○ If you are checking a single file, click on the **Add Files icon** in the menu bar, navigate to and select the desired file and then click on the **Open button**.



   ○ If you want to check all the files contained within a directory, click on the **Add Folder icon** in the menu bar, browse and select a drive or directory and then click on the **OK button**.



6. A list of files appears with 64-character strings next to them. These are the SHA256 checksums.
7. Verify that the checksum generated by the *HashMyFiles* tool matches the checksum published by Kanguru Solutions.

11.1 SHA256 Checksum Values

If the checksum generated by the *HashMyFile* tool matches the checksum published below, then your files are genuine.

Defender client downgrader tools

Device	File name	SHA256 Checksum value
Defender Elite200 Cloud	KDME200_CC_Downgrader_Cloud.zip	3ed1c13b1f1e03024cc1401ac97d23c41dd15c10b8bef0287cfad2bb51a5a1cb
Defender Elite200 Enterprise	KDME200_CC_Downgrader_Enterprise.zip	4c12fc4313a32cee1967e7958a45c15cfb44158878d4eab21a434c78c59c389b
Defender Elite200 No-Comms	KDME200_CC_Downgrader_No-Comms.zip	8686fb8267e49f2f94f7d5d4a5051467ff84390990d343597edac9c7bf83c9bb
Defender 2000 Cloud	KDM2000_CC_Downgrader_Cloud.zip	cbb5f4b1b3a8f3fab6c732686a2abf9cf3ba49c176686647cb2a7976ea69dff0
Defender 2000 Enterprise	KDM2000_CC_Downgrader_Enterprise.zip	37de2a6e34a8479eab5d7f29bc2414892d81815f501df2229e6e8b38749684c3
Defender 2000 No-Comms	KDM2000_CC_Downgrader_No-Comms.zip	32d9f626e8965e5cbea2d924d78775fe170c9f822211f27370a7aab93d3135fb

UKLA and KRMC installer files

Software	File name	SHA256 Checksum value
UKLA	UKLA_v3.2.0.3_setup.zip	44f1091561ef5f4d131a0f6fd98df10dee6905c64f3bacc6e661acefa1134ae9
KRMC	KRMC 5 Server 5.0.2.6.zip	4d8fa1a41012090b0f7194a8b931e23ca79196b15a068b886bf938bf58366789

User Manuals and Product Guides

Document	File name	SHA256 Checksum value
UKLA User Manual	UKLA User Manual v3.2.1.pdf	2b2abf0f619d8c2623aed5ec973cbf1fc3c6228d8b937cd1f62f355dbcb9af65
KRMC Installation Guide	KRMC - Enterprise Edition - Install Guide v5.pdf	f0d2e21e5c1490c29ca6663fe5a80533e892f7b7c7f065959c5127dc8c31bbc1
KRMC Install Sheet	KRMC - Enterprise Edition - Install Sheet v5.pdf	f983e94db3adc4f3bec4bdc0ac33d4cb1aba84b57ba115ec90725f4e42fca16f
KRMC Super Admin Guide	KRMC - Enterprise Edition - Super Admin Guide v5.0.2.pdf	b6d07847ec38e28517e22026eefe29d94e1a7bbb8d3215acdc027f29fc0bbd24
KRMC Admin User Manual	KRMC - Enterprise Edition - Admin User Manual v5.0.2.pdf	d79dcd21e3faa19e94dda66643aa01d2081855808fc3e2a8dd4639ed1b3547ce
Defender Elite200 User Manual	Kanguru Defender Elite 200 User Manual v1.1.1.pdf	9f09870b70cee6397f5337877cc9653160947801d8b194a72fc5ccee080e137a
Defender 2000 User Manual	Kanguru Defender 2000 User Manaul v1.1.5.pdf	5700b1e601c0e575892caa3abc4edee54e0874e9d44f1b9a4a67b02a9391bab2

(Continued on next page)

Defender 2000 Cloud Edition Client Application Files (KDM2000 v 1.2.1.8 -2)

File name	SHA256 Checksum value
KDM2000	cfe4236c88133c863693555a7f77eca09a727359b700981c18c6b72d4049e115
KDM2000.exe	f6d1823e316e92bda6f1a06cf91c1f354d116106b901445897f247ced2ff5ed4
autorun.inf	ce93f4e4337eda6b52e0cac8eef760565ce985639aa2d4a5c58ad5f65ae5584a
enlogMacLnx.sh	bd2e68ecabd72063e875328971ffbc3980d0910d6ce34dc26d24774e5091c699
enlogWin.bat	8cc34684b6714cec9b23f5a20f7d27ddc079ec972b289d951830c355e47e5455
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
kdm2000_exec.sh	2bc65f6557d283f618ad1cfdce8771c009e91d28c14d1347386196166c34e0c1
version.ini [1, 2]	eaabaed0f28dd58cec97d51b0db8334096709029525e32b0a121ab563ef23740
KDM2000.app\Contents\Info.plist	3583351073de26fc9377f30f8df4c20b3ddb27cd31966347f11f27bd4689506e
KDM2000.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDM2000.app\Contents\MacOS\KDM2000	d3d10dd417298c98a7b7e4a4e71f6b2f3c1c5ac593ad4c57b7e95a78accbbaaa
KDM2000.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDM2000.app\Contents\Resources\empty.lproj	

[1] For a Kanguru Defender 2000 (Cloud Edition) CC-certified at the time of purchase.

[2] For a non-CC certified Kanguru Defender 2000 (Cloud Edition) migrated to a CC certified version using the CC downgrade tool provided by Kanguru, the SHA256 hash for the version.ini file is:
6fdce4d2b0a877633978dd2a54332ebd80532521a841c257950d4e0a57b05503

Defender 2000 Enterprise Edition Client Application Files (KDM2000 v 1.2.1.8 -3)

File name	SHA256 Checksum value
KDM2000	73e0370fd9bdfdc7bc182cc049ba4ad56939525ab2a7d2872609ef55550443d3
KDM2000.exe	ea91d11336561c6c7c605f3d41c060a53f39cdc908482f585fc98e7fee0f6bd4
autorun.inf	ce93f4e4337eda6b52e0cac8eef760565ce985639aa2d4a5c58ad5f65ae5584a
enlogMacLnx.sh	bd2e68ecabd72063e875328971ffbc3980d0910d6ce34dc26d24774e5091c699
enlogWin.bat	8cc34684b6714cec9b23f5a20f7d27ddc079ec972b289d951830c355e47e5455
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
kdm2000_exec.sh	2bc65f6557d283f618ad1cfdce8771c009e91d28c14d1347386196166c34e0c1
version.ini [1, 2]	1b4a1a252ad6e3c13c6e621fbb35ef34934243477afc1e21b04e999f233b0a54
KDM2000.app\Contents\Info.plist	3583351073de26fc9377f30f8df4c20b3ddb27cd31966347f11f27bd4689506e
KDM2000.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDM2000.app\Contents\MacOS\KDM2000	cc4cef38f6648295fb24d342b64a7f5f5302de1dc66f3390d5b72bae95bc0e3d
KDM2000.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDM2000.app\Contents\Resources\empty.lproj	

[1] For a Kanguru Defender 2000 (Enterprise Edition) CC-certified at the time of purchase.

[2] For a non-CC certified Kanguru Defender 2000 (Enterprise Edition) migrated to a CC certified version using the CC downgrade tool provided by Kanguru, the SHA256 hash for the version.ini file is:
6fdce4d2b0a877633978dd2a54332ebd80532521a841c257950d4e0a57b05503

Defender 2000 No-Comms Edition Client Application Files (KDM2000 v 1.2.1.8 -6)

File name	SHA256 Checksum value
KDM2000	8f313a05556d7b80fd84d66ff41e7414fddcdb19593c0fd3f16b202608b76a79
KDM2000.exe	6d62fa2f02b5245ec4ea15099729e7b44a6367488c2f7a14fee2a60c6a05278c
autorun.inf	ce93f4e4337eda6b52e0cac8eef760565ce985639aa2d4a5c58ad5f65ae5584a
enlogMacLnx.sh	bd2e68ecabd72063e875328971ffbc3980d0910d6ce34dc26d24774e5091c699
enlogWin.bat	8cc34684b6714cec9b23f5a20f7d27ddc079ec972b289d951830c355e47e5455
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
kdm2000_exec.sh	2bc65f6557d283f618ad1cfdce8771c009e91d28c14d1347386196166c34e0c1
version.ini [1, 2]	cfca0dabebe27f763de9800b65c7ff670cfc51b74d4a7e84c70810b63e5bb2f1
KDM2000.app\Contents\Info.plist	3583351073de26fc9377f30f8df4c20b3ddb27cd31966347f11f27bd4689506e
KDM2000.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDM2000.app\Contents\MacOS\KDM2000	50baf92470f61cee1d4511151e0af534122238d71120300305a8cbf458224cc5
KDM2000.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDM2000.app\Contents\Resources\empty.lproj	

[1] For a Kanguru Defender 2000 (No-Comms Edition) CC-certified at the time of purchase.

[2] For a non-CC certified Kanguru Defender 2000 (Enterprise Edition) migrated to a CC certified version using the CC downgrade tool provided by Kanguru, the SHA256 hash for the version.ini file is:
408079e9ee7598a2e81065b6c9a0e543b14853616ef0cdd1f774acc9658b9f73

Defender Elite200 Cloud Edition Client Application Files (KDME200 v 2.0.0.0 -2)

File name	SHA256 Checksum value
KDMElite200	7aaa053034da6862ae06f0863e716a8add8a6c6a306f0e47c35d379eb80c2b8a
KDMElite200.exe	1ae42409ee184c0c63cd8a07ceb238dc698b2b005313b65f66f57c4aee6d8bb2
autorun.inf	e039edbcbd56f630a0f91b2736206a21e1654e928cf7e0e46636a3ec2a8d4fe8
enlogMacLnx.sh	90df28ab8d2b8810d3543e336c2861be2d275a4c1e8f3f540cd811efa11c32d4
enlogWin.bat	35d006f87e455a691bbbc3a06ec90eceb133d7dedac43f7145c3eb90400f57c2
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
version.ini [1, 2]	dce6a73d2875cef5bc07250bf017e65b297064ff4f0372e95b0ec86ada0a5ac8
KDMElite200.app\Contents\Info.plist	ea4f922841c1cb95f4cf6ba0ff3ec707d17fbaf32a624af09786be51de221d7d
KDMElite200.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDMElite200.app\Contents\MacOS\KDMElite200	a839cc84a55899dfc456e4579499274675dac15cc9fe99ca402cc241a5517923
KDMElite200.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDMElite200.app\Contents\Resources\empty.lproj	

[1] For a Kanguru Defender Elite200 (Cloud Edition) CC-certified at the time of purchase.

[2] For a non-CC certified Kanguru Defender Elite200 (Cloud Edition) migrated to a CC certified version using the CC downgrade tool provided by Kanguru, the SHA256 hash for the version.ini file is:
a9d648bde5e1c8baa35943de0966d4066f85bb8c4c0f251d87ac4372205b3182

Defender Elite200 Enterprise Edition Client Application Files (KDME200 v 2.0.0.0 -3)

File name	SHA256 Checksum value
KDMElite200	c03eed99ad8a2e7e86e0f4cfc54c4d4746c41bfa3ee39a990471bf235d5e1c24
KDMElite200.exe	b6e69610c222d7fb5cfbb9aac2cd4ace8e5f6710e43ccaa2f2efca53fa85e49b
autorun.inf	e039edbcbd56f630a0f91b2736206a21e1654e928cf7e0e46636a3ec2a8d4fe8
enlogMacLnx.sh	90df28ab8d2b8810d3543e336c2861be2d275a4c1e8f3f540cd811efa11c32d4
enlogWin.bat	35d006f87e455a691bbbc3a06ec90eceb133d7dedac43f7145c3eb90400f57c2
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
version.ini [1, 2]	6347a2c9ff9cb53a39f615815af4cbc165176f09cedef6e04f2678d6b054e272
KDMElite200.app\Contents\Info.plist	ea4f922841c1cb95f4cf6ba0ff3ec707d17fbaf32a624af09786be51de221d7d
KDMElite200.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDMElite200.app\Contents\MacOS\KDMElite200	f1e4c5113784f3ca459fa3083cf75a65110cd75df5958c63326cf7993341b2f6
KDMElite200.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDMElite200.app\Contents\Resources\empty.lproj	

[1] For a Kanguru Defender Elite200 (Enterprise Edition) CC-certified at the time of purchase.

[2] For a non-CC certified Kanguru Defender Elite200 (Enterprise Edition) migrated to a CC certified version using the CC downgrade tool provided by Kanguru, the SHA256 hash for the version.ini file is:
892dac017567d0b8d797820fd972226f0c558711a6e99382a30b2ad46676a4a5

Defender Elite200 No-Comms Edition Client Application Files (KDME200 v 2.0.0.0 -6)

File name	SHA256 Checksum value
KDMElite200	129d1216a10540647e2479d4ae0ca736c66b0fab8548a1fbefa8ef406dadc7e8
KDMElite200.exe	f829fc65b315e4093ad102c7eb3e1a1140e73f45b78b29f2e3b749a8f405c0d2
autorun.inf	e039edbcbd56f630a0f91b2736206a21e1654e928cf7e0e46636a3ec2a8d4fe8
enlogMacLnx.sh	90df28ab8d2b8810d3543e336c2861be2d275a4c1e8f3f540cd811efa11c32d4
enlogWin.bat	35d006f87e455a691bbbc3a06ec90eceb133d7dedac43f7145c3eb90400f57c2
iconKDM.ico	d7720c8f0f11a15cb33733ffcee8838d5ea017276ca8e0740b9eeab2dd4676c2
version.ini [1, 2]	f11472b29d041ea434f05b2a8374b42908a63edc2e403f335199443298fa8110
KDMElite200.app\Contents\Info.plist	ea4f922841c1cb95f4cf6ba0ff3ec707d17fbaf32a624af09786be51de221d7d
KDMElite200.app\Contents\PkgInfo	7e50a30efad50208a173203ced60818d693bb61266b75aa10927d1a2adce80cb
KDMElite200.app\Contents\MacOS\KDMElite200	10392d37e6e5ebcd68ef0e29b5be34fba45be0e4f6aea8837de657d3f631c9f1
KDMElite200.app\Contents\Resources\KDMElite.icns	ea1587ff8f13dbf549c03a3fa2b34652050abdfb6cdb0c99492f945bf748838e
KDMElite200.app\Contents\Resources\empty.lproj	

[1] For a Kanguru Defender Elite200 (No-Comms Edition) CC-certified at the time of purchase.

[2] For a non-CC certified Kanguru Defender Elite200 (No-Comms Edition) migrated to a CC certified version using the CC downgrade tool provided by Kanguru, the SHA256 hash for the version.ini file is:
65ad17a0e5a566d879ede6a3bc5581c0d1a50036cad1aa24efb87f16c7deba88

12. Changelog

v1.3 updated 5/30/2013

- Updated CC certified client version of KDME to 2.7.1.9
- Updated CC certified client version of KDM1000 to 1.0.1.1
- Updated CC certified client version of KDM2000 to 1.2.1.8
- Added Instructions for identifying the different Defender models
- Added instructions for checking for tampered/broken seals
- Added instructions to check device firmware version as a user requirement
- Added download links for KRMC and UKLA
- Added download links for Enterprise edition client updaters
- Added certificate verification for client updaters in Windows
- Added certificate verification for KDMElite client application in Windows
- Added chapter on Defender Elite and 1000 write protect switch
- Added Changelog

v1.4 updated 6/06/2013

- Inserted instructions for verifying SHA256 checksum of KRMC and UKLA installer files

v1.5 updated 7/16/2013

- Added available capacities for each Defender model

v1.6 updated 12/11/2013

- Removed Defender 1000 and Defender Elite models
- Added Defender Elite200 model
- Added Defender Elite200 user manual and client updater download links
- Added CC certified versions of KDME200 client application and firmware
- Updated Kanguru logo

v1.7 updated 3/11/2014

- Included the write protect switch in section 2.10 Excluded functionality

v1.8 updated 3/31/2014

- Disabled ability for the client to automatically download updates if configured specifically for CC
- Added notification about the system administrator’s responsibility to ensure that the client version is in compliance with common criteria

v1.9 updated 5/13/2014

- Added note that directs the user to instructions on checking their device’s client version
- Phrase “Use of those features is not permitted in evaluated configuration” replaced with “these features have not been evaluated as part of the CC configuration.”
- Added notification that Defender devices may not come with CC compliant client pre-loaded with link to section on updating the client version.
- Added notification that Defender devices may not come with CC compliant client pre-loaded with link to section on updating the client version.
- Added Mac as an OS that does not support checking the digital certificate.

v1.10 updated 6/16/2014

- Updated links for Standard and Enterprise client version upgrader/downgraders
- Updated links for UKLA and KRMC Enterprise install software
- Added SHA256 Checksum values for digital distribution packages for KRMC and UKLA and Defender clients
- Added images and description of tamper evident stickers that are affixed to packaging

v1.11 updated 7/17/2014

- Consolidate all hash checking to a single chapter
- Change the Hash tool used to Hashmyfiles.exe
- Add SHA hashing for KRMC, UKLA and Defender user documents
- Add hash for individual files on Defender's CD-ROM partition
- Add note that the Device Control module was not evaluated for CC and must not be enabled
- Add note to check the hash of individual files on secure partition
- Note that going from non-CC KRMC to CC certified version requires a fresh install and instructions for installing previous non CC KRMC
- Add to Device downgrade process and note to check for any physical evidence of tampering and reset the drive before applying the update
- Note that KRMC Cloud functionality must remain disabled
- Updated links to document and updater downloads
- Removed 2GB version of Defender Elite200

v1.12 updated 8/06/2014

- Added instruction that user must verify the files on the CD-ROM partition against the checksums in chapter 11 after performing a device update

v1.13 updated 8/12/2014

- Add instructions for verifying and updating No-Comm edition devices
- Add instructions for downloading client downgrader for No-Comms devices
- Add SHA256 hashes for No-Comms devices

v1.14 updated 8/18/2014

- Add instructions for checking product version number listed in the version.ini file to identify whether device is Cloud, Enterprise or No Comms edition

v1.15 updated 8/19/2014

- Add -2, -3 and -6 versions of KDM to software requirements in sections 2.4, 5.0 and 5.2
- Add KDM version numbers to SHA256 Hash tables in section 11.1

v1.16 updated 8/27/2014

- Add section 4.4.2 for identifying the KDM Client edition (i.e. enterprise, cloud or no-comms) and differences between editions
- Section 4.4.3 add possible upgrade paths for different client editions
- Section 11.1 updated user manual versions Defender 2000 and Elite 200.
- Section 11.1 updated hash values of updated Defender 2000 and Elite 200 user manuals.

v1.17 updated 9/19/2014

- Section 4.4.2 KDM Cloud edition device users must disable anti-virus on their devices

v1.18 updated 9/23/2014

- Section 4.4.2 KDM Enterprise edition admins must disable anti-virus on their devices

v1.19 updated 9/24/2014

- Revised client version numbers for Defender Elite200 and Defender 2000 in Section 11.1

v1.20 updated 10/2/2014

- Updated the file names in the SHA256 Checksum tables for Defender Elite200 Clients and Defender 2000 Clients

v1.21 updated 12/4/2014

- Add 02.05.10 to list of approved firmware versions for Defender 2000 and Elite200 in Section 2.3 and Chapter 5
- Update SHA256 Checksum for Defender Elite200 and Defender 2000 User Manual in Section 11.1

KANGURU™

Secure. Anytime. Anywhere.

Kanguru Solutions
1360 Main Street
Millis, MA 02054
www.kanguru.com

Legal terms and conditions available at www.kanguru.com. Please review and agree before use. Thank you.