Kanguru Solutions SED30 and SED300 User Manual

Version	Published
1.0	March 2024
2.0	May 2024

3.0	August 2024

Introduction	
What is an SED?	
Why use hardware-based encryption?	
Meet the software	
Before Initializing Security on your new SED	
How would you like to use it?	
Configuring your bootable SED	
1. Test your computer's boot compatibility	
Initialize Testing with a different hard drive	٤4
Initialize Testing with a USB drive	4
2. Backing up any data is recommended	4
3. Install your Operating System	4
4. Disable Sleep Mode	4
5. We recommend Updating your BIOS firr	nware4
6. Installing Opal Commander	4
6. Running Opal Commander	
7. Activating Security	9
Unlocking the drive through the Kanguru Pre-B	oot Authenticator12
Configuring your drive for storage (non-bootab	e)13
Running Opal Commander	
1. Activating Security	

Introduction

What is an SED?

The Kanguru SED product line is a self-encrypting hard drive capable of full disk encryption to prevent unauthorized access to your computer at rest. Unlike most encryption types, this process activates security across the entire storage disk. Access to data requires authentication credentials, even before reaching the Operating System.

The SEDs come in 2 form factors, NVMe M.2 and 2.5" SSD SATA, allowing for a wide range of compatible computer systems.

Why use hardware-based encryption?

All encryption types are not created equal; there are several benefits to hardware-based encryption. One is that in the case of Kanguru SEDs, the encryption key does not leave the hardware, it is generated internally and never exported. Another is that typically hardware-based encryption is faster than software-based encryption and not dependent on outside processes for performance. In most cases, there is no conflict between hardware encryption and software encryption; meaning a user can have both running in parallel.

Meet the software

The application used to manage security, encryption, and configuration of the SEDs is called Opal Commander. It's a Windows and Linux installable program capable of initializing the Kanguru SED product line as well as making changes to the drives such as Username, Password, and installing our PBA (Pre-Boot Authenticator).

Before Initializing Security on your new SED

How would you like to use it?

Your SED can be used as a bootable drive, capable of running an operating system and securing your workstation's data at rest. The SED can also be used as a storage drive, using Opal Commander, the drive can be locked and unlocked at will for external use if desired. If you are planning to use the drive internally as a bootable disk, continue to the section labelled "Configuring your bootable SED". If you are planning to use the drive as either internal or external storage (non-bootable), continue to the section called "Configuring your SED for storage".

Configuring your bootable SED

There are some safety measures that we would recommend you perform before initializing security on your drive. Please follow these steps and you're on your way to initializing your self-encrypting drive for bootable use.

1. Test your computer's boot compatibility

Some computers prefer UEFI bootable options while others use Legacy BIOS configurations. It's important to keep your BIOS up to date and try Kanguru's Pre-Boot Authenticator before initializing security. Kanguru's PBA supports both UEFI and Legacy boot options, but to be safe, please test one of the following:

Initialize Testing with a different hard drive

If you have a hard drive with an OS capable of running Opal Commander, try initializing the SED without an OS or data. This will allow you to install the drive to your PC and test that your BIOS will support either the UEFI boot or Legacy boot options provided. Make sure you can reach the login GUI of the Pre-Boot Authenticator. If the unlock is successful, you can turn off security and install your new operating system and enjoy using your new encrypted drive.

Initialize Testing with a USB drive

If you have a USB drive that you can use to create bootable media, we recommend trying to create a bootable USB version of the Kanguru PBA. After installing Opal Commander, use the Kanguru PBA ISO or IMG file to create a bootable USB.

2. Backing up any data is recommended

If the SED you're working with already has critical data on it, you can initialize security and begin the encryption process without wiping any data. We recommend backing up any/all data in case errors occur or you need access to your data during the initialization process.

3. Install your Operating System

The SED30 and SED300 work as normal hard drives before encryption is enabled. It is easier to install your preferred operating system before enabling encryption. If you already have an operating system installed on your drive, you can skip this step.

4. Disable Sleep Mode

When you enter sleep mode, the SED locks itself for safety purposes. This can be a problem if you're using it for your internal operating system drive. We recommend turning off sleep mode and using alternative options.

5. We recommend Updating your BIOS firmware

The Pre-Boot Authentication feature runs by booting from the BIOS, often using UEFI. Make sure your BIOS firmware is up to date by downloading the latest flash update from your system's manufacturer.

6. Installing Opal Commander

Opal Commander is available on our support site here: <u>https://kanguru.zendesk.com/hc/en-us/articles/25912797815821</u>

The default installer is for Windows, but specific flavors of Linux installers can be provided upon request.

To install, follow these steps:

- 1. Double click the Opal_Commander_Setup.exe (usually a version number is applied to the end of the executable name).
- 2. You will be prompted with an End User License Agreement (EULA), if you agree to the terms listed, choose "I accept the Agreement" and click "Next".



 There are additional settings in the next window, you may choose to "Create a desktop shortcut" or "Automatically start Opal Commander" when you login to your operating system. Make your choices and click "Next" to continue.

Setup - Opal Commander version 1.1.2.1		—		×
Select Additional Tasks Which additional tasks should be performed?			((III)
Select the additional tasks you would like Setup to perform while ins	talling Opal Commande	er, then dic	k Next.	
Additional shortcuts:				
Create a desktop shortcut				
Startup:				
Automatically start Opal Commander				
	Back	Next	Car	ncel

4. If you are ready to install Opal Commander, select "Install" at the next window.

Setup - Opal Commander version 1.1.2.1		_		×
Ready to Install Setup is now ready to begin installing Opal Commander on your com	puter.		(
Click Install to continue with the installation.				
	Back	Install	Can	cel

5. The installation will progress with a loading bar and take you to the last window. You may choose to launch Opal Commander right away or simply click "Finish" to complete the installation process.

🛃 Setup - Opal Commander version 1.1.2.1	X
	<text><text><text></text></text></text>
	Finish

6. Running Opal Commander

Opal Commander is an application designed to initialize full disk encryption on any Kanguru hard drive that is Opal TCG 2.0 compliant.

Opal Commander							-	- 🗆 X
KANGURU [™] Secure. Anytime. Anywhere.							v0.0.13.1	About
 ✓ I Drive Details View All 	Drive Information	ı						
✓ ☺ Locking Lock Unlock				G Ref	iresh			
Ø Drive Management	Kanguru DS300N	_		Driv	e name: N/A			
Security Secure Boot Drive and User Info	Good	77°F 25°C	Drive ID PhysicalDrive2	Interface USB ATA	Serial number KNSNV01211100009	FW ver ECPM13.0	MBR Locking Disabled	Admin N/A
,	Drive Health	Temperature	Capacity 512GB	Opal ver Opal 2	FIPS Supported	Security Inactive	MBR Shadowing N/A	User N/A

- 7. Activating Security
- 1. Start Opal Commander by clicking the designated shortcut on your desktop or running the Opal Commander application from your start menu.
- 2. In the navigation menu on the left, choose the "Security" option.
- 3. The Security information appears in the right pane of the window.

Commander			- 🗆 X
KANGURU [™] Secure. Anytime. Anywhere.		v0.0.13.	1 About
 Image: The second second	Security Initialize a drive to activate security, Activate security to enforce password authentication. Suspend security to disable password authentication and Secure Boot.		
Security Security Secure Boot Drive and User Info Reset To Factory			
	Select drive: No Drive selected		G Refresh

- 4. Use the "Select drive" drop menu to choose the drive you would like to initialize security on.
- 5. Click "Secure Initialization", the Secure Initialization window will appear.

Sopal Commander			- 0	×
Secure. Anytime. Anywhere.	·	0.0.13.1(About	
 Invice Details View All O Locking Lock 	Security • Initialize a drive to activate security. • Activate security to enforce password authentication. • Suspend security to disable password authentication and Secure Boot.			
Onick Onick Onick Security Secure Boot Drive and User Info Reset To Factory	Select drive: No Drive selected	· (G Refres	ih
	PhysicalDrive2 - Kanguru DS300N - 512GB - KNSNV01211100009 - USB ATA - ECPM13.0 - N/A			

- 6. Name the device for the application's use, as well as create an Administrator Username and Password. All configuration changes made to the device from now on will require the Administrator Password.
- 7. Optionally you can create a standard user, this user will be able to lock and unlock the drive but cannot make any settings changes.
- 8. If you plan on using this device as an internal hard drive with an Operating System, you'll need to install the PBA image Kanguru provides. This PBA will allow you to boot into a login screen on system power and allow you unlock your OS by using the Administrator's credentials or the User's credentials. You can find your specific PBA image on our Opal Commander's download page. There is 1 for NVMe drives and 1 for SATA drives.

Secure Initialization	\times	Secure Initialization		×
Drive Name:		Drive Name: Kangur	u-Test	
_ Admin		Admin		
Name:		Name:	Admin	
Password:	Ø	Password:		2
Re-enter Password:	8	Re-enter Password:	•••••••	2
Create User		Create User		
		Name:	Optional	
Password:	Ø	Password:		2
Re-enter Password:	Ø	Re-enter Password:		2
Enable Secure Boot		Enable Secure Boo	t	
PBA Image: ler\kanguru_pba.iso Browse		PBA Image: ler\kangi	uru_pba.iso Browse	
Drive Name is empty.				
OK Cancel			OK Cancel	\mathbf{D}

9. Please be aware, the Secure Boot PBA installation can take up to 30 minutes. This is the most intricate section of the process that will allow a user to login to the device through a Pre-OS Environment. Giving your drive complete encryption at rest with the ability to unlock using simple credentials. The loading screen may sit at 66% for a long duration, that section of the process takes the longest.

PhysicalDrive2.FullInitialization progress	×
Loading PBA Ima	ge.
	66%

10. When the installation is completed, the drive will be left in the unlocked state to prevent the OS from crashing during a lock.

Opal Commander								- 0 ×
Secure. Anytime. Anywhere.							v0.0.13.1	About
✓ ☐ Drive Details View All	Drive Informatior	1						
✓ ② Locking Lock				G Ref	resh			
 Ø Drive Management 	Kanguru DS300N			Drive name:	Kanguru-Test			
Security Secure Boot Drive and User Info Reset To Factory	Good Drive Health	77°F 25°C Temperature	Drive ID PhysicalDrive2 Capacity 512G8	Interface USB ATA Opal ver Opal 2	Serial number KNSNV01211100009 FIPS Supported	FW ver ECPM13.0 Security Active	MBR Locking Enabled MBR Shadowing Enabled	Admin Admin User Optional

11. Your drive has activated its security, your drive is now encrypted and in the unlocked state. The drive will remain unlocked until you cycle the power. Note: All drives will remain unlocked until locked through Opal Commander or the device is power cycled.

Unlocking the drive through the Kanguru Pre-Boot Authenticator

If you chose to install the Kanguru PBA, your SED is now a bootable drive. Capable of launching into Kanguru's pre-boot login screen to unlock your drive and load your operating system.

Here is the process to unlock a PBA installed drive:

- 1. Be sure to install your SED into your computer as an internal drive. The SED can be used as a bootable drive through an external USB connection, but the boot sequence will be related to USB configuration instead of internal.
- 2. Turn on your computer.
- 3. Access the BIOS by using the keyboard shortcut your manufacturer recommends, often the ESCAPE or DELETE buttons.
- 4. Navigate to your boot sequence options and choose to boot from your new Kanguru SED as the primary boot option.
- 5. Save and Exit the BIOS.
- 6. The Kanguru PBA will load into a menu with the following options.
 - a. Boot GUI fast
 - b. Boot GUI slow
 - c. Boot Terminal fast
 - d. Boot Terminal slow
- 7. When the interface loads, you will see the Kanguru PBA login window in the center. It has fields for choosing which drive to unlock and to input the user's password.
- 8. If you have a mouse, use the mouse to click the dropdown menu and choose the SED you'd like to unlock. If you don't have a mouse, use the arrow keys to choose your SED and press TAB to enter the password field.
- 9. Provide your password for the chosen SED and press ENTER.
- 10. The PBA will now begin to close and load your operating system since the drive is now unlocked.

Configuring your drive for storage (non-bootable)

Running Opal Commander

Opal Commander is an application designed to initialize full disk encryption on any Kanguru hard drive that is Opal TCG 2.0 compliant.

Solution Commander							-	- 🗆 X
Secure. Anytime. Anywhere.							v0.0.13.1	About
 Z Drive Details View All 	Drive Information	1						
✓ ⊘ Locking Lock				G Ref	iresh			
 Ø Drive Management 	Kanguru DS300N			Driv	e name: N/A			
Security Secure Boot Drive and User Info Reset To Factory	Good	77°F 25°C	Drive ID PhysicalDrive2	Interface USB ATA Opal ver	Serial number KNSNV01211100009 FIPS	FW ver ECPM13.0 Security	MBR Locking Disabled	Admin N/A User
	Drive Health	Temperature	512GB	Opal 2	Supported	Inactive	N/A	N/A

- 1. Activating Security
 - 1. Start Opal Commander by clicking the designated shortcut on your desktop or running the Opal Commander application from your start menu.
 - 2. In the navigation menu on the left, choose the "Security" option.
 - 3. The Security information appears in the right pane of the window.

🛃 Opal Commander			- 🗆 X
Secure Anytime Anywhere.		v0.0.13	.1 About
 Image: Second state of the second	Security Initialize a drive to activate security. Activate security to enforce password authentication. Suspend security to disable password authentication and Secure Boot.		
v view Management view Manag			
·	Select drive: No Drive selected		G Refresh

- 4. Use the "Select drive" drop menu to choose the drive you would like to initialize security on.
- 5. Click "Secure Initialization", the Secure Initialization window will appear.

Solution Commander		- 🗆 ×
KANGURU [™] Secure. Anytime. Anywhere.	v0.	0.13.1 About
 ✓ I Drive Details View All ✓ Ø Locking Lock Unterk 	Security • Initialize a drive to activate security. • Activate security to enforce password authentication. • Suspend security to disable password authentication and Secure Boot.	
Security Security Secure Boot Drive and User Info Reset To Factory		
	Select drive: No Drive selected	G Refresh
	Secure Initialization	

6. Name the device for the application's use, as well as create an Administrator Username and Password. All configuration changes made to the device from now on will require the Administrator Password.

- 7. Optionally you can create a standard user, this user will be able to lock and unlock the drive but cannot make any settings changes.
- 8. Make sure to leave the PBA checkbox UNMARKED, your intention is to make this drive a nonbootable storage drive. Enabling the PBA will cause the drive to install Kanguru's Pre Boot Authenticator and the drive will act like a bootable OS hard drive.

Secure Initialization		×
Drive Name:		
- A due in		
Admin		
Name:		
Password:	Ø	
Re-enter Password:	Ø	
Create User		
	Ø	
	Ø	
Enable Secure Boo	ot	
Drive Name is empty.		
	OK Cancel	

9. Once you click OK, your drive is now initialized and encrypted. The drive will remain unlocked as to prevent access until you turn off the power or disconnect the drive.