

SanDisk – Cruiser® Enterprise

SecureWave Certification Number: CERT-SDC-07-03-0027

Cruzer® Enterprise is a USB drive specifically designed to meet the unique security, compliance, and manageability needs of enterprise-size businesses. It does not rely upon users to decide which files to secure. Instead it requires mandatory access control for all files, storing them in an encrypted, password-protected partition. This ensures security and protects stored data in the event of device loss or theft. Cruiser Enterprise features ultra fast transfer speeds, a simple interface, and the ability to plug-and-play. It's intuitive and practical enough for users to start using immediately. With hardware based encryption and mandatory access control, Cruiser Enterprise helps IT managers more effectively protect information on company issued portable storage devices.

- > Hardware based 256-bit AES encryption
- > Mandatory access control for all files (100% private partition)
- > Strong password
- > "Lockdown" mode when a set number of incorrect password attempts are made
- > Centrally Manageable (Using SanDisk CMC software sold separately)
- > Ultra fast transfer speed – 24MB/s Read, 20MB/s write.
- > Available in 1, 2, and 4GB configurations

For more information, please visit:

[http://www.sandisk.com/OEM/ProductCatalog\(1340\)-Cruzer_Enterprise.aspx](http://www.sandisk.com/OEM/ProductCatalog(1340)-Cruzer_Enterprise.aspx)



Sanctuary Device Control

Sanctuary® Device Control extends the enforcement of enterprise policies to I/O devices. Users can access only explicitly authorized devices, such as SanDisk's Cruiser Enterprise. Sanctuary Device Control manages this by applying an Access Control List (ACL) to each device type. To grant access, the administrator need only associate user or group objects to the authorized device.

Sanctuary® Device Control supports several directory platforms, including Microsoft Active Directory and Novell eDirectory. Sanctuary has also been ported to Windows Embedded platforms in addition to the Windows Server and Desktop versions. Sanctuary Device Control:

- > Ensures USB Security through management of any removable media,
- > Provides complete control and management over all I/O devices through any port including USB, Firewire, WIFI, Bluetooth, etc.,
- > Prevents data theft and data leakage via removable media,
- > Prevents malware introduction via removable media,
- > Audits I/O Device usage,
- > Detects and blocks Keyloggers,
- > Encrypts removable media that may not provide their own hardware based encryption,
- > Enables Regulatory Compliance with enforceable policies that include extensive logging and auditing,
- > Provides centralized logging and retention of an exact copy of all data written to authorized devices using SecureWave's proprietary Shadowing™ technology.

For more information, please visit: www.securewave.com/sdc

Request a free 30 days fully enabled evaluation at www.securewave.com/evaluation

Enforcing data security policies is made easy with SanDisk Cruiser® Enterprise secured device. Combined with Sanctuary® Device Control, organizations are equipped with the way to enforce the use of a secured hardware based encrypted device while protecting against the risk of data leakage from the use of unauthorized or unsecured devices including keyloggers.

SecureWave Sanctuary[®] provides policy-based control over endpoint applications and devices. Using an automated whitelist approach, Sanctuary enables the development, enforcement, and auditing for application and device use in order to maintain IT security, reduce the effort and cost associated with supporting endpoint technologies, and ensure compliance with regulations. Sanctuary links application and device policies to Microsoft[®] Active Directory[™] or Novell[®] eDirectory[®] user and user group information, dramatically simplifying the management of endpoint application and device resources. More than 1,800 enterprises worldwide in the financial, government, military, manufacturing and healthcare sectors utilize Sanctuary. SecureWave, named a Red Herring Top 100 Innovator, is headquartered in Luxembourg and services its global customer base via offices in the U.K., Washington D.C., and a network of reseller and service provider partners worldwide.

More information about SecureWave Technology Partners: www.securewave.com/alliances/
Locate a SecureWave Sanctuary Official Channel Partner: www.securewave.com/channel/



SecureWave
Safeguarding Tomorrow

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America

+1 (703) 713-3960 Phone
+1 (703) 793-7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom

+44 (0) 1908 357897 Phone
+44 (0) 1908 357600 Fax

Continental Europe

Atrium Business Park
23 Rue du Puits Romain
L- 8070 Bertrange
Luxembourg

+352 265364-11 Phone
+352 265364-12 Fax

www.securewave.com
info@securewave.com

SECUREWAVE SANCTUARY CERTIFIED