

Table Of Contents

Table Of Contents 1

IRONKEY ENTERPRISE & BASIC S1000 FREQUENTLY ASKED QUESTIONS

What are the available capacities for the S1000?

The S1000 is available in a 4GB, 8GB, 16GB, 32GB, 64GB or 128GB configuration. 1GB = 1,000,000,000 bytes.

How fast is the S1000?

Blazing fast with read speeds up to 400MB/sec and write speeds up to 300MB/sec. You can stream any video with zero delay.

Will the S1000 work in my computer's USB 2.0 port?

Yes, the S1000 is a USB 3.0 device and it is backwards compatible with USB 2.0. However, you will not see the increased speed that USB 3.0 offers.

My computer has a USB 2.0 port; will I get the benefit of these faster speeds?

No, if you are using a USB 2.0 port, then you will see the standard USB 2.0 speeds and not see the benefit of the S1000's faster read and write speeds. We are continuing to ship the S250 and D250 for users that have a USB 2.0 port. However, the S1000 allows you to future proof as USB 3.0 becomes more prevalent. There is no plan to EOL the S250 or D250 at this time.

Does the S1000 use SLC flash like the S250?

No, the S1000 uses MLC flash. The S stands for Secure Storage, and is not representative of SLC flash

Will the IronKey S1000 replace the IronKey S250?

No, the S1000 is perfect for users that have a USB 3.0 port on their computer and require the faster speeds that USB 3.0 provides. If your system has a USB 2.0 port then the S250 or D250 is the ideal device providing speed, security and a ruggedized design.

Why is the S1000 priced the same as the S250?

The S1000 and S250 are for different user needs. If you are a power user and your computer has a USB3 port than S1000 is the perfect solution. The S250 is the ideal solution if your system has a USB2 port.

What Operating Systems does the S1000 support?

The S1000 is compatible with Microsoft Windows 10, XP SP2+, Vista, Windows 7, Windows 8/8.1, Windows Server 2008, Macintosh OSX 10.5+, and Linux 2.6+.

What is the difference between AES CBC Mode and AES XTS Mode?

AES XTS provides more protection than the other approved confidentiality-only modes, such as CBC, against unauthorized manipulation of the encrypted data such as plaintext and watermark attacks. CBC mode breaks data into blocks and uses a different encryption key for each block sequentially. AES XTS is equivalent to double encryption of the text, using two different keys. Both are approved by FIPS 140-2 Level 3 but XTS is recommended for stronger security.

Does the S1000 support the same applications as the D250 and S250 series of devices?

Only the IronKey Anti-Malware Scanner is available on the S1000 Enterprise devices.

Can I upgrade a Basic S1000 to an Enterprise S1000?

Yes, the process to upgrade the Basic S1000 to an Enterprise S1000 can be performed through the IronKey Control Panel. The device can only be activated with the IronKey Enterprise Cloud Management Service or On-Premises Server of which your organization must already be a subscriber. If you have any questions or trouble with your device, please contact your system administrator.

Can I manage S1000's with IronKey Enterprise Management Service or Server?

Yes, you can manage enterprise devices with the IronKey Enterprise Management Cloud Service or On-Premises Server. Each device needs a management service license.

What do I need to install the IronKey Anti-Malware application on my S1000 device?

The IronKey Anti-Malware service is only available through IronKey Enterprise Cloud Management Service or On-Premises Server. In order to install anti-malware, your company needs to have IronKey Enterprise Management, and the device must have a valid management license and Antimalware subscription. Once the enterprise account is properly licensed, an IronKey administrator can enable the service through policy.

Can I change an Enterprise managed drive to a Basic drive?

No, an Enterprise device cannot be switched to become a Basic device since this could open up security vulnerability. Furthermore, once a Basic device has been upgraded to an Enterprise device, it cannot revert back to a Basic model even after resetting or reassigning the drive through IronKey Enterprise Cloud Management Service or On-Premises Server.

Do the Silver Bullet Remote Administrative features work on Enterprise S1000s?

Yes, all Silver Bullet features are supported through the Enterprise Management on the S1000 Enterprise model.

How can I recover my password?

As part of the security of the device there are no "backdoor" passwords or ways for IronKey to restore the device for you.

IronKey Basic S1000 What if I can't recall my password?

After 10 failed consecutive password attempts, the device will either reset or permanently self-destruct based on this setting. This feature is configured at the time the device is initially set up and can be updated in the Preferences menu of the IronKey Control Panel. The reset function will wipe all your data and the AES Encryption keys on your device, so your data will not be recoverable, but allows you to initialize and use the device again. **Please note:** this option must have already been set within the IronKey Control Panel. Without unlocking the device there is no way to change from self-destruct to reset.

IronKey Enterprise S1000

IronKey Enterprise S1000 users may contact their IronKey Enterprise Administrator for password assistance.

Can I send my device to IronKey to recover my data?

No. Not only do we not have the ability to access your device, but this would be a security flaw and defeat the purpose of a secure device.

Can I send my device to you for a replacement if I forgot my password?

The lifetime IronKey S1000 hardware warranty covers hardware manufacturing defects. Devices with forgotten passwords or that have self-destructed are not eligible for replacement because the product worked as designed.

Does the S1000 protect against BadUSB?

IronKey Secure USB devices, including the S1000, are not vulnerable to BadUSB malware. For more information please visit the following link: <http://ironkey.com/en-US/solutions/protect-against-badusb.html>

Can government agencies access my IronKey S1000 with a master password?

No, the S1000 is designed to be the world's most secure flash drive. Without the password, the data on the device is not accessible. As part of the security of the device there are no "backdoor" passwords, or ways for IronKey to access the device.

Why does the S1000 have an S prefix?

The 'S' stands for Secure Storage, just as the 'W' stands for Workspace and 'H' stands for Hard Drive.

Is the IronKey S1000 bootable?

No, the IronKey S1000 must be unlocked in a supported operating system as listed above. For bootable IronKey devices, please see our family of Windows To Go certified drives.

