Kleberg Since 1905 Bank

IronKey Trusted Access - FAQs

What is an IronKey Trusted Access device?

The IronKey Trust Access device is a portable USB device that allows users to access a secure virtual environment from any computer. This virtual environment is then able to help protect users from malware attacks that could compromise private information.

How do I start using IronKey Trusted Access device?

We require that you complete a configuration form to define the parameters of your computer and network for device setup.

We then deliver a pre-configured IronKey thumb drive that you insert into a USB port on your computer. The device installs components to improve security, initiates a reboot and you then log in to Online Banking through the IronKey hosted Internet Browser, resulting in a secure Online Banking experience. Anytime you want to Bank with us, you just activate the device with a secure password and it will launch a browser to your Bank's website.

How does IronKey Trusted Access work?

IronKey Trusted Access invokes its own operating system and secure internet browser, along with encrypting both the keyboard and information being displayed on the screen. This combination of security layers prevents criminals from stealing personal information or Online Banking login IDs or passwords. This approach does not require use of the existing operating system or browser, which could be infected. Even if the host system is infected with malware, Ironkey Trusted Access will not be affected.

How does IronKey Trusted Access work with my existing Cash Management cookie?

When you install the device for the first time, the Cash Management cookie is reset through Online Banking support and installed on the IronKey Secure Access device. From that point forward, you are not able to access Online Banking Cash Management without the use of the device. This prevents unauthorized access to your Cash Management functions.

What host operating systems does IronKey Trusted Access support?

Trusted Access for Banking supports 32-bit versions of Windows XP, Vista, and 7 along with the 64-bit version of Windows 7. The device also requires at least 2 GB of system memory.

Can I use the IronKey Trusted Access device on any computer?

This device can be used on any computer that meets the minimum requirements. It is possible to install the device in multiple systems so you can access and perform Online Banking functions from home or work. To install the drivers you need to have Administrative rights to the computer, and we discourage the use of public computers (Library, Coffee Shop, etc.) for any use in which information may be stolen.

How does keyboard input encryption work?

IronKey Trusted Access secures keyboard input from the Windows keyboard driver through to the virtual operating environment. Windows APIs, applications, or malware attempting to intercept keyboard input will receive encrypted ciphertext.

Does Trusted Access for Banking require any server hardware or software?

Trusted Access for Banking does not require server hardware or software. All deployment and policy management is performed through the IronKey Enterprise Management Service operated by IronKey.

Are updates or integration with banking applications required to use Trusted Access for Banking?

Trusted Access for Banking does not require special application integration or modifications. Existing web-based Online Banking applications are accessed using the Secure Browser.

Can I access my IronKey Trusted Access system through a remote access session such as Log-Me-In, or PCAnywhere?

No, If a user is logged in remotely (e.g. log-me-in) then the Trusted Browser will not accept keyboard input (though mouse input does work). Our browser will only accept input from our keyboard driver. This is by design to ensure a hacker cannot manipulate a session remotely. In addition, even if the user does try to enter the login and password, it will not be displayed and most keyloggers will not pick up the keystrokes due to the basic protection of the solution. It is NOT recommended to attempt to use this device through remote sessions.

What happens when my device times out due to inactivity? Can I just leave it in my USB port?

The session will be terminated, and you can leave the device in the slot without excess risk, but to be safe, we advise that this device be unplugged when not in use.

What happens if the IronKey Trusted Access for Banking device is lost or stolen?

If the device is lost or stolen and someone tries to access it through the password protected login screen it will self destruct if the user exceeds the number of attempts (typically set to 3-5 tries). It will also self destruct if they try to cut into the device to access the internal chip. If the device is lost or stolen please contact us and we will remotely destroy the device to protect your banking information (the Cash Management cookie) and replace the device with a new one. We can also track the device to see where it is being plugged in to determine the approximate location of its use.