Landmark Bank

IronKey Trusted Access – Frequently Asked Questions

Landmark Bank has partnered with IronKey, Inc., an Internet security company, to offer the "Trusted Access" security device. These Frequently Asked Questions (FAQs) are intended to help explain the solution to you. If you still have questions, please contact your Landmark Bank Business Services Officer at (800) 618-5503.

What is the IronKey Trusted Access Solution?

IronKey Trusted Access provides a safer environment for conducting online business banking by utilizing a portable USB security device to store a tamper-proof virtual environment that runs completely separate of other applications on a computer. Trusted Access allows a connection to the Landmark Bank website through a secured tunnel that keeps banking safer, even if a computer is compromised by a virus. When using IronKey Trusted Access the secure tunnel is intended to help protect the computer so malware can't tamper with the browser or redirect to a fraudulent or counterfeit site, and its anti-fraud technology is designed to secure input from the keyboard so malware can't log keystrokes.

How does IronKey Trusted Access work?

By plugging the IronKey device into the USB drive of the computer, the Trusted Access application invokes its own operating system and secure Internet browser, along with encrypting both the keyboard and information being displayed on the screen. While we cannot promise any technology to be 100% fail proof, this combination of security layers is designed to prevent criminals from stealing personal information. This approach does not require use of the computer's existing operating system or browser, which have the risk of being infected. Even if the host computer is infected with malware, Ironkey Trusted Access is designed to not be affected. Think of Trusted Access as a standalone secured computer running side-by-side the host computer.

How do I start using the IronKey Trusted Access device?

We require that you complete a **Pre-Install Questionnaire** to define the parameters of your computer and network for device setup. This questionnaire outlines the system requirements that you will need to validate before installation of the device can be completed. Upon receiving your new IronKey Trusted Access device, you will walk thru some initial activation steps to install the Trusted Access application and create a device password, which is explained in an easy-to-follow End User Guide we will be delivering with each device.

During initial activation, the device installs components to improve security and initiates a reboot of the computer (*note: some computers may require a shut down vs a reboot*). From that point forward, you will log into Internet Banking using the USB device and IronKey's hosted browser to establish a secure connection for your online banking session. This process takes about 30 seconds and while that may seem like an additional delay in getting to our website, it is helping keep your accounts safer.

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

Prior to your activation of the Trusted Access device, Landmark Bank will reset your Cash Manager cookie. Then when you log into Internet Banking the first time using IronKey Trusted Access, the cookie will be installed on the IronKey device. From that point forward, you are not able to access Internet Banking Cash Manager without the use of the device. This prevents unauthorized access to your cash management functions.

What will I notice that will be different when using the IronKey Trusted Access device?

As with any additional security layer, there will be slight changes to the way you will perform banking functions. You will notice slight differences in fonts during some functions such as file upload menus and save menus. This is ok and normal.

Printing, exporting and capturing screen shots (saving) will change slightly. The End User Guide will include screen shots to explain each step. Other functions such as Paperless Statements & Notices and Bill Pay will work as usual.

Navigating to websites within the Trusted Access browser will only be allowed for bank-approved sites (the white list). It is important to always use IronKey Trusted Access when logging into Internet Banking, as any other browser could lead to loss of confidential data.

What systems does IronKey Trusted Access use?

VirtualBox Project powers the virtual environment with a Tiny Core Linux operating system and Mozilla Firefox browser. IronKey, Inc. maintains, tests, and qualifies the version of VirtualBox and Tiny Core Linux included with Trusted Access.

How does keyboard input encryption work?

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

What are the System Requirements for Trusted Access to work?

- ☐ **Operating systems** supported include Windows XP, Vista, or Windows 7*
- ☐ **Minimum of 2 GB RAM** required
- ☐ **Network Connection** – wireless and DSL may slow down the device performance (dial-up may not work at all)
- ☐ **Local Administrator rights** are required during the initial driver installation only.
- ☐ **Network Security Settings:** If there is a **network proxy** in place or a **web filter**, you will need to allow for IronKey to communicate through these systems:
    - ○ **Proxy Settings** – Does your business or location utilize proxy settings for accessing the Internet? If yes, you may need to involve your IT administrator or consultant at implementation.
    - ○ **Web Filtering –** Does your business or location utilize Web Filtering? If yes, please provide the following IP Address to your IT administrator or consultant, because it will need to be added to your Whitelist (allowed URLs) policy: ***.ironkey.com. 70.42.140.0/24, 74.201.87.0/27, 74.201.121.0/27**

**Mac Users: IronKey is currently developing an upgrade that will be Mac compatible.*

Is IronKey Trusted Access compatible with the following?

Adobe PDF Reader or Plug-In	Yes
JavaScript	Yes
Cookies	Yes
Printing	Yes, saves file as a PDF on the computer’s desktop
Saving	Yes, saves file as a PDF on the computer’s desktop (note: this device is not intended as a general purpose storage device)

Are we required to use the IronKey device?

The answer will depend on your company’s functionality entitlements and setup for Internet Banking. Please contact your Business Services Officer for further discussions.

Can we use the device on more than one computer?

YES, you can use it at work or at home. It just requires an initial installation to take place, like any other software application does, and then you will be able to plug it into any computer that has been set up. And the good news is that the Internet CFO® Cash Manager ‘cookie’ will be placed on the device, so it will travel with you.

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

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). The browser will only accept input from the browser's 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 key loggers 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.

Can more than one user share a device?

Yes, the IronKey device does not store any Login ID's or passwords, so you can share devices if necessary, A few items to mention, if applicable:

1. Because this is a security system, we will <u>assign the device to one person</u> and only grant support for device administration (e.g. reset the password) to that assigned individual.

2. We strongly recommend a minimum of <u>two (2) IronKey devices per business</u> to minimize the risk of not having access to Internet CFO® Cash Manager (e.g. employee on leave, device left at home or lost) when ACH or Wire Transfer origination needs to be completed, as well as to allow for recommended security procedures such as dual authorization or separation of duties.

3. A business owner only needs one device if they own more than one business and have multiple Internet CFO logins.

Are there any fees for the IronKey Trusted Access solution?

Yes. We are offering this solution at a nominal fee. Please contact your Business Services Officer for more information.

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

Immediately call **Landmark Bank at (800) 618-5503**. Please note that there is a lost or stolen device replacement cost of $250 per device, should a new device be required.

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 a specific number of attempts. We can track the device to see where it is being plugged in to determine the approximate location of its use. The device will also self destruct if they try to cut into it to access the internal chip.

- **Lost Devices** – If the device is lost, we will disable the device. This does not destroy it, but renders it unusable until we enable it to work again. We will replace the device with a new one.

- **Stolen Devices** – If the device is stolen, we will remotely detonate the device to protect your banking information (the cash management cookie). The next time the USB device is plugged into a computer, the device will self-destruct. If the device is relocated before it has been plugged into a computer, we are able to reverse the detonation so that it is not destroyed. We will replace the device with a new one.