WEB-key Client
Installation and Use Guide

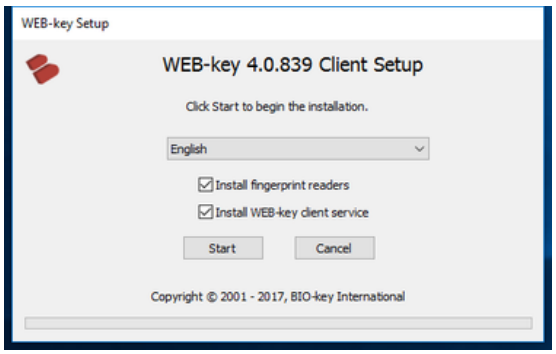
Version 4.0

Summary:

This document outlines the process of installing and configuring the WEB-key client for biometric authentication into applications and systems. Follow these simple steps for easy use and installation of the system.

Installation:

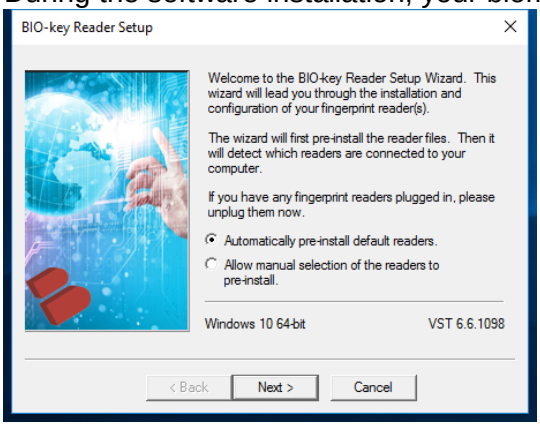
There are two key steps to installing the WEB-key client. First is the software, then the hardware (biometric readers). Be sure that the software is installed before the hardware is plugged in, or the Windows Plug-n-play software will fail to find the correct drivers.



You must first install the WEB-key client software to load the appropriate drivers for the hardware (biometric readers). Installing the hardware first may cause the hardware configuration to fail, and cause the drivers to not load correctly until a reboot is accomplished. Install the WEB-key client software in a couple of ways. You may have an application (WEB-keySetup_04_00_xxx.exe), or you may download the client from a web page enabled to do so.

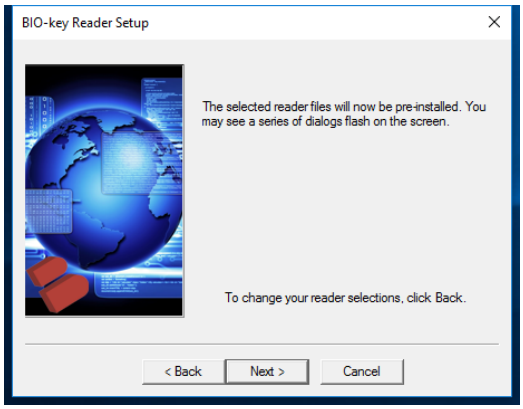
It may take it a couple of minutes to download the installation program, based on the network connection speed.

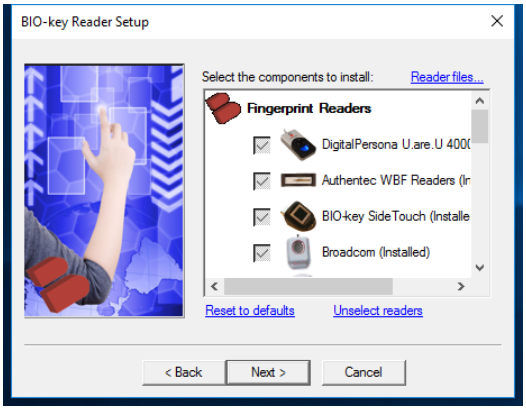
During the software installation, your biometric reader may be automatically configured.



The installation program will ask you to plug in the biometric device, if it is an external USB style device. Follow any Found New Hardware Prompts to properly install the device. If the Wizard requires any drivers, point it to the "C:\Program Files\BIO-key\Drivers" directory. From that point Windows Plug-n-Play should find the correct drivers and install them. Wait about 30-60 seconds for the process to complete successfully.

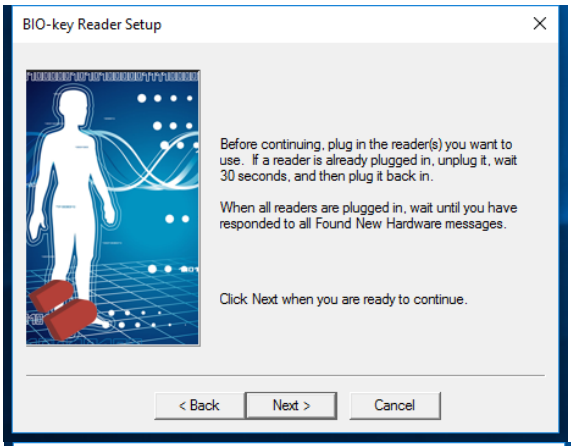
Not all reader installation applications are 'silent' on their installations. The default checks in WEB-key denote the ones that silently install. The others may have pop-ups asking for confirmation or settings. The VST Reader Install and Setup Guide provided further details on which reader installs can be automated, which operating systems they support and other special items to know.

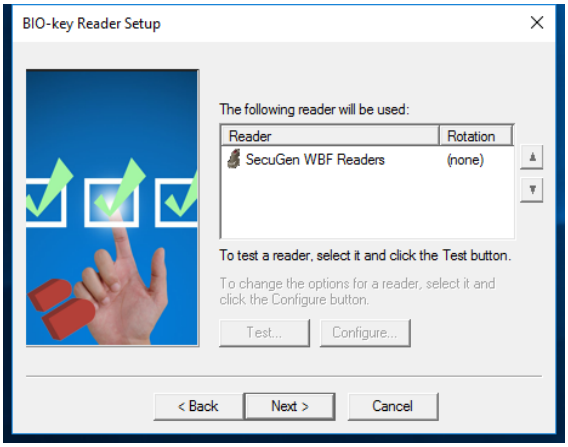


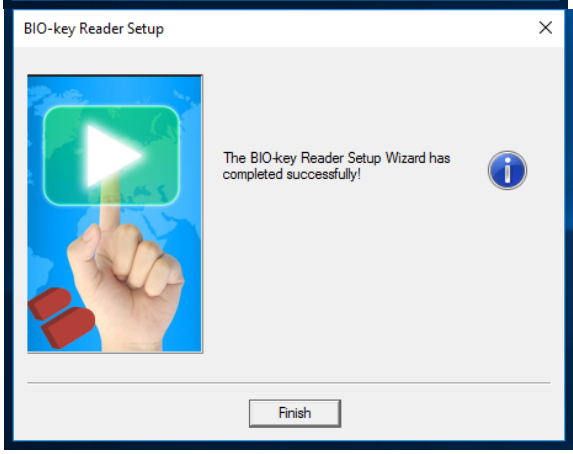


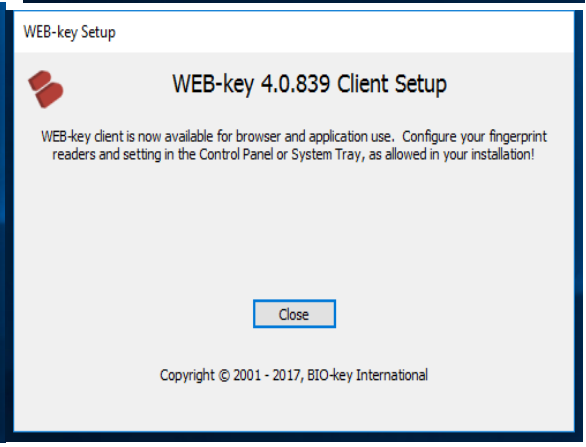
Once it is installed, let the install program auto-discover its type and configure it for use. It will go through each possible device type and 'look' for the device and initial functionality. Following that search a list of connected readers will be displayed. Typically this is only a single device (biometric reader), but it is possible to connect more than one as well, but they must be of different types (brands).

The final dialog of the Wizard will list the readers that are found. If yours is not found, unplug it, plug it into a different port, wait 60 seconds and then hit 'back' and 'next' to try again. The list can be ordered to pick which reader is defaulted as first. Only one reader will be initialized and used, the others are fall back readers to use of the first is not available. This is helpful for laptops with docking stations. Use USB reader if tethered, and use the internal reader if undocked. It gives great power for no additional configuration needs.



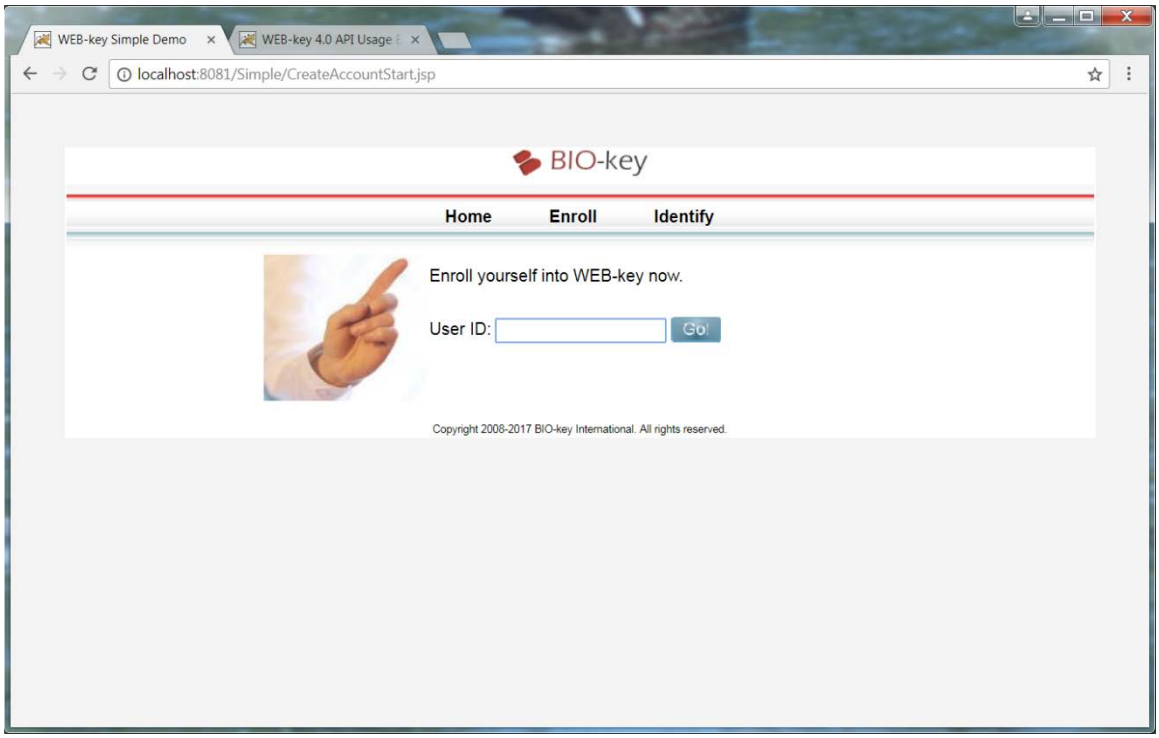


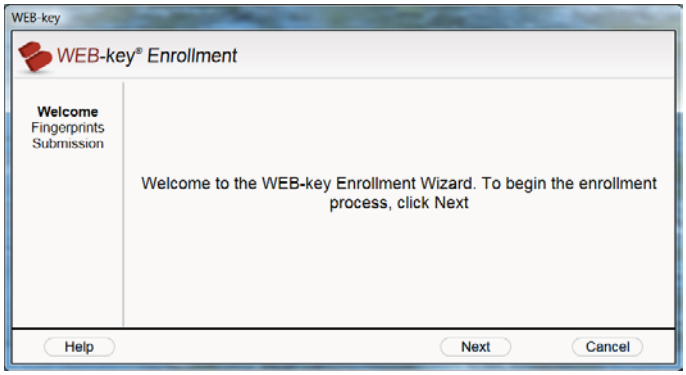




Enrollment:

The first step in using WEB-key with a specific application is to enroll your of finger or fingers. "Enrollment" means that you register ‘mathematical’ templates of your fingers for use in identifying you later. You will identify yourself to the application whenever you begin a secure activity. Your application may and will look different, but the flow and general elements are the same. WEB-key can operate in many different Web and windows, Android and iOS based applications, and the look and feel of the control can change with custom ‘skins’.



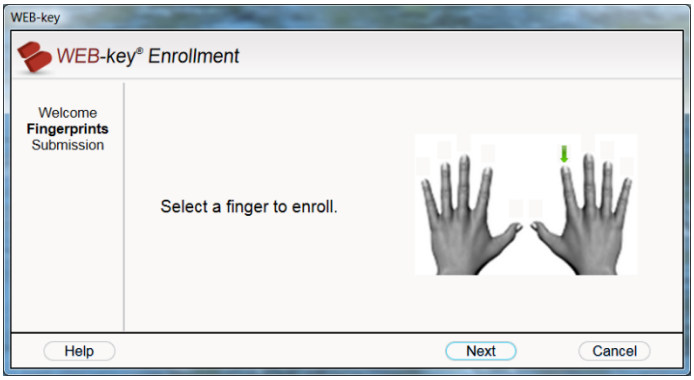


Click on the Enrollment start area of the screen to begin the process. Depending on how your site is configured it may or may not ask for other information. Most often the Enrollment code step is skipped. But if not, here is a summary.

During enrollment, you may be asked for an enrollment code and another unique identifier (user ID, or similar number) for the application. The application administrator provides you with this information prior to enrollment. If you received an enrollment code and an application identifier, make sure that you have them on hand.

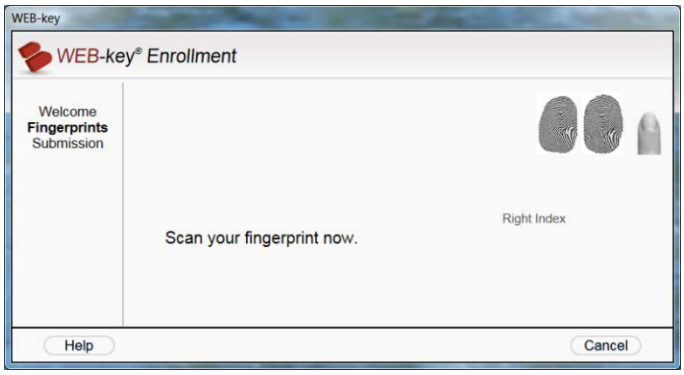
An enrollment window may display if the application requires an enrollment code and another unique identifier along with your enrollment finger templates. The enrollment code and identifier protect your identity by ensuring that the fingers you enroll actually belong to you. The enrollment code is valid for one enrollment only. Once it is used, it is done and gone.

Enter the enrollment code carefully, exactly as it was provided to you. The enrollment code can contain up to four sections separated by dashes. Use all CAPITAL letters for the enrollment code. Do not type dashes. Press <Tab> to move from one section of the code to the next.



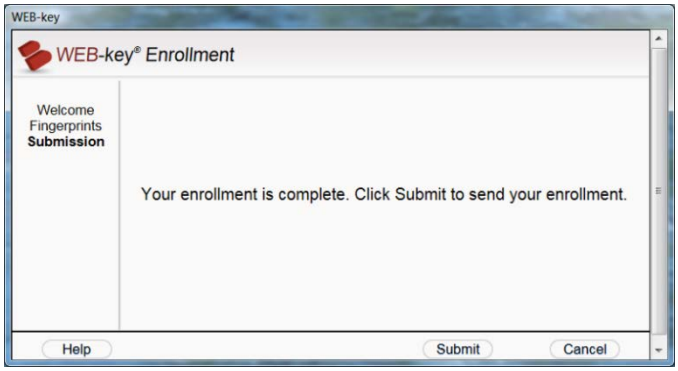
Next, this window allows you to indicate which finger you want to enroll. You can enroll up to 10 fingers based on the application set limits, and each finger will be scanned at least 3 times. The Web application determines the number of fingers that their users enroll. WEB-key automatically asks for the required number of fingers. Some fingers can be disabled due to missing or poor quality prints. Do this by right clicking on the finger being displayed that you wish to 'disable'.

Enrolling multiple fingers allows you to continue identifying yourself when one of your fingers is injured. In fact, it is a good idea to enroll at least one finger on each hand, in case a hand or arm injury prevents you from using the finger reader on one side.



This window allows you to scan the finger that you just selected for enrollment. WEB-key provides visual cues and messages to help you get the best possible scan.

The finger that you selected is scanned at least three times. After three successful scans, WEB-key compares the scans to determine if they are similar enough for later identification purposes. If not, WEB-key requests additional scans to be taken. This assures the best results.



When the enrollment process is complete and all the data is validated, the confirmation screen is displayed. This will send the biometric enrollment data to the server, and or to the client device to be stored for later use. Failing to click 'submit' here will lose all the enrollment data. You must click 'submit' to send it.

When you submit the enrollment to the application, the process is complete. WEB-key will record your information, keeping it protected and private. You can now use the finger biometric to access the application successfully.

Fingerprint Quality:

Fingerprint scan quality can affect the reliability of any electronic finger identification system. WEB-key identifies you by creating a mathematical finger model based on the features of your finger that make them unique. Thus, it is important that your scans be clean, high-quality, and consistent. This topic describes the characteristics of a good finger scan and explains how to achieve them.

Some fingers scan better than others. The index fingers, middle fingers, and ring fingers usually produce the best scans. The thumbs and little fingers are difficult to place properly on the scanner. And thumbs are often more scared or worn than other fingers.

When you scan your finger, the center of your print should be at the center of the scanning surface. WEB-key helps you to position your finger by displaying the following visual cues:

The image viewer shows the live print image currently captured by the reader. This image changes as you move your finger on the scanning surface.

The red target in the middle of the image viewer shows where the center of your print should be.

Blue cross hairs appear at the center of your fingerprint. The best scan occurs when you align the cross hairs within the red target circle.

The way that you place your finger on the reader is critical to scan quality. The four factors of good finger placement are:

- Centering your finger
- Applying correct pressure
- Avoiding movement
- Consistency

Centering your finger: Place the center of the flat area of your finger flat against the center of the scanning surface. Do not raise your finger so that only the tip is scanned, and do not rotate your finger so that only one side is scanned.

Applying correct pressure: Apply light to normal pressure against the scanning surface. Excess pressure distorts your fingerprint by forcing the ridges to merge. Press as you would when dialing a phone or typing on a computer keyboard.

Avoiding sliding movement: Place your finger on the reader in a single downward motion. Once placed, avoid dragging your finger across the scanning surface to center your print. To reposition, lift your finger completely from the reader and place it back down again.

Consistency: Scan your finger the same way every time. It is critical to get good scans when you enroll into the system. After enrollment, use the same finger placement that you used for enrollment.

The condition of the skin on your fingers can affect the quality of the finger scan. You can resolve some of these problems before scanning your finger.

Dry fingers can produce an incomplete or broken image. Dryness can be caused by a lack of natural moisture in the skin, by environmental conditions, or by handling substances that absorb or neutralize the skin's oils.

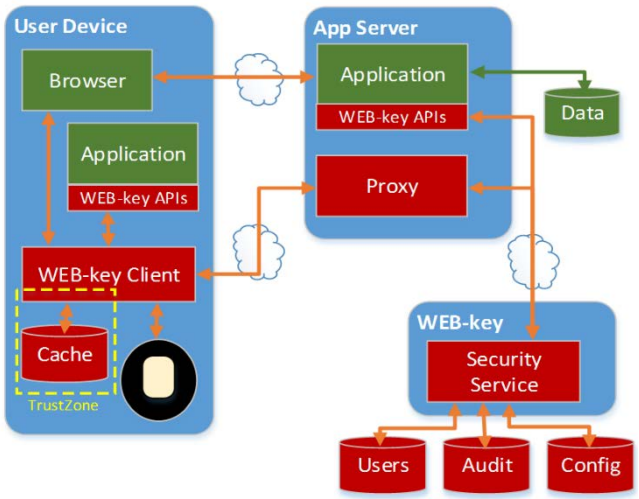
Regenerate the skin's natural oils by rubbing your fingers against the palm of your hand or against your forehead or the side of your nose. This will add moisture.

Wet fingers can produce a muddled image. Wet prints can be caused by sweat or by handling wet or oily substances such as food or lotion.

Dry your fingers with a towel, cloth, or even a piece of clothing.

WEB-key System Architecture:

The WEB-key Architecture is a series of building blocks for a complete Client Server solution. This guide covers the client side configuration and basic operation of the system. The server side is left for the system administrators and separate guides.



On the client, the components are rather simple. There is a physical device, a biometric fingerprint reader that scans and passes a user fingerprint through drivers that are often USB plug-n-play enabled to a driver. The driver is built by the company that produced the biometric device.

Today BIO-key supports dozens of different vendor's hardware for fingerprint capture. Each has differing drivers, benefits and costs. The device drivers used must be the ones supplied with the BIO-key software you are using. In some cases many versions of these device drivers are available, but not all are applicable to use due to changes in the drivers that cause incompatible use.

The core of the client is the WEB-key ClentService executable. Browsers communicate with client by launching a small BrowserHandler executable. As a DLL client service could be incorporated into traditional Windows and Java applications. Clients are also available for Android and iOS. The one installation will install all required elements for the various connections possible to many applications. As a user you can setup which reader it to be used at install, or via a Control Panel applet for configuration and maintenance. Web application can detect which version of the control is present and request that a new version update the current one. This process is automatic to the users. Only applications that are configured to use WEB-key can take advantage of the power, security and ease of use it provides for authentication.

The primary files for the WEB-key client reside in C:\Program Files\BIO-key\WEB-key 4.0 and C:\Program Files\BIO-key\Common. Other files are placed into C:\Windows\System32 and related areas as required for drivers or registration purposes. There is an uninstall capability in the Control Panel. This will remove all WEB-key control elements, but not the drive drivers. We assume other applications may be making use of device drivers, and it is not good practice to remove them.