



# BioPassword®

## Questions and Answers

**Q-1 What is BioPassword®?**

**A-1** BioPassword is a patented software-only security solution that uses keystroke dynamics; a technology based on biometrics, to accurately identify an individual by the way he or she types.

**Q-2 How does BioPassword work?**

**A-2** BioPassword uses patented biometric technology to capture the individual keystroke rhythm that uniquely identifies an individual. This rhythm, combined with the user's password, generates a "hardened password." Layering this hardened password on your existing security framework provides a multi-factor authentication solution. This solution effectively shields your entire network from unauthorized access.

**Q-3 Why should I add BioPassword to network security measures already in place?**

**A-3** Today's organizations must use an integrated security strategy to protect critical network resources. BioPassword is a software-only solution, so it integrates seamlessly with existing network security strategies as well as future plans to add items such as smart cards or tokens. The patented BioPassword "hardened password" technology provides a strong, durable layer of secure protection at a very low total cost of ownership.

**Q-4 How can BioPassword help me with regulatory requirements?**

**A-4** BioPassword helps meet the challenges of regulatory requirements by preventing unauthorized internal and external network access and by providing audit trails. More information on this, as well as details on HIPAA, Graham-Leach-Bliley, or Sarbanes-Oxley legislation, can be found at [www.biopassword.com](http://www.biopassword.com).

**Q-5 How convenient is BioPassword to use for legitimate users?**

**A-5** BioPassword is unobtrusive, allowing end users to access the system in their normal way, by typing in their designated password. The only new step is the enrollment process: an individual provides a series of typing samples to train BioPassword to recognize his or her unique typing rhythm. BioPassword remembers that rhythm so that the next time the user logs on, that individual can be authenticated as an authorized user.

**Q-6 What are biometrics and why use them for user authentication?**

**A-6** A biometric is a unique, measurable characteristic or trait of a human being that can be used to verify identity. Biometrics are well suited for user authentication because they can confirm an individual's identity by examining a unique physiological trait or behavioral characteristic.

**Q-7 What is strong user authentication and how does BioPassword provide it?**

**A-7** Strong user authentication occurs when an individual is required to provide more than one form of proof of identity. BioPassword requires individuals to provide something they know (a password), and something they do that is unique to them (their typing rhythm).

**Q-8 What is keystroke dynamics?**

**A-8** Keystroke dynamics is a biometric that accurately identifies an individual based on their unique typing rhythm.

**Q-9 Do people really have a unique way of typing?**

**A-9** Yes. Whether the user is a “hunt and peck” or 120-words-per-minute typist, BioPassword can distinguish an individual’s unique typing rhythm.

**Q-10 Can BioPassword address ALL my user authentication needs?**

**A-10** No. BioPassword is only one piece of the security and user authentication puzzle. BioPassword is a software-only technology that can work with existing password policy and security processes. It is an added layer of security that raises the threshold of strong authentication at a small incremental cost.

**Q-11 What business problems does BioPassword solve and where can I apply it?**

**A-11** BioPassword strong user authentication technology addresses three primary business purposes:

- Policy-based information asset protection where specified levels of security can be assigned to groups of users or individuals for different levels of network access control either at the workplace or remotely.
- A mechanism for compliance with mandated regulations and standards, such as HIPAA and FTC consumer protection, to minimize corporate liability.
- Process efficiency and cost savings in business-to-business (B2B) and business-to-consumer (B2C) relationships

**Q-12 How accurate is BioPassword?**

**A-12** All internal and external testing of BioPassword indicate that BioPassword can meet industry requirements for false rejects (when the correct user is denied access) and false accepts (when an imposter is allowed access). This accuracy assumes that the “imposter” is given a legitimate username and password and is given an unlimited number of attempts to gain entry. If BioPassword is combined with normal security procedures, such as locking out potential intruders after 3 failed attempts, then the accuracy improves dramatically and approaches 100%.

**Q-13 Why is BioPassword important to network security and other environments that use passwords?**

**A-13** BioPassword is designed to avoid the problems associated with using traditional password security, such as internal security breaches, social engineering, password-cracking programs, and employee negligence. By providing a completely new layer of protection, BioPassword restores integrity to the password as the most convenient and cost effective means of network, data, and transaction protection and saves organizations the time and trouble associated with adopting expensive and potentially intrusive hardware technology. BioPassword eliminates the problems associated with casual sharing of passwords between individuals in the workplace. Further, individuals with malicious intent cannot easily use passwords protected by our keystroke technology, even with sophisticated password cracking tools. For some companies, password resets or rotation can be reduced or eliminated depending on the needs and policies of that organization.

- Q-14** What if I need to wear gloves or a bandage, I hurt my hand, or if I injure a finger?
- A-14** BioPassword has the flexibility to accommodate minor changes in your typing rhythm. The network administrator can modify the security setting or disable BioPassword to allow you to access the network. If your typing style has permanently changed, the network administrator can delete your old template and you can then re-enroll.
- Q-15** Does BioPassword log keystrokes? Is it a keystroke logger?
- A-15** No. A keystroke logger captures the keys you press and stores them for later retrieval. BioPassword stores only the timings created by a user's personal typing rhythm. Therefore no data is provided to a keystroke-logging device. If a keystroke logger is used to collect the username and password keys, BioPassword nullifies that data because only the legitimate user can match their own personal typing rhythm.
- Q-16** Does BioPassword prevent hackers from stealing user account/ passwords (using software such as L0pht Crack/Pwdump 1,2,3/Sam Grab)?
- A-16** No, however, if hackers steal your SAM/Active Directory hashes and decrypt them, they will fail to gain access. Even though the stolen user name and password information is correct, the biometric template will not be. Access will be denied.
- Q-17** What if someone develops a program that steals the keystroke biometric templates along with username/password accounts?
- A-17** Such an effort would not be successful because BioPassword contains technologies specifically designed to thwart the efforts of hackers.
- Q-18** How can I try BioPassword on my Windows network to be sure it works as you describe?
- A-18** Please contact our sales department at [sales@biopassword.com](mailto:sales@biopassword.com). They can assist with providing a fully functional evaluation copy of BioPassword. You can also request an evaluation copy from our website, [www.biopassword.com](http://www.biopassword.com).
- Q-19** Does BioPassword for Enterprise Networks eliminate the need for password rotation?
- A-19** Our recommendation is to maintain all your existing network security procedures, and to follow the guidelines published by the National Institute for Standards and Technology (NIST). Specifically, the Federal Information Processing Standard (FIPS), number 190, "Guideline for the use of advanced authentication technology alternatives" advises organizations to practice a 120-day rotation in password policy. For additional information, go to [www.nist.gov](http://www.nist.gov).
- Q-20** What is the enrollment process and how long does it take?
- A-20** Enrollment by an end user takes about 1 to 3 minutes. A user types their username and password multiple times to create a stored template. Once complete, the user is advised that they are enrolled and ready to log on normally.



Software-Only Strong User Authentication

- Q-21** What if we have the need for greater security? Are there any settings we can adjust to increase security?
- A-21** Yes, the network administrator can globally change the security threshold settings for all users or for any individual depending on specific needs. These changes can be permanent or temporary. The security thresholds are set up in a simple scale from 1 to 100 to make changes quick and easy.
- Q-22** What if I use a laptop that is not always connected to the network?
- A-22** BioPassword allows users to access their laptop while it is disconnected from the network and still protects it from any unauthorized access.
- Q-23** Can more than one person have their BioPassword template on a single workstation?
- A-23** Yes, they can. When multiple users share a single workstation, users simply log on in their usual way, using their network profiles. The network operating system authenticates each user by their user name and password and BioPassword authenticates each person by their typing rhythm. Only one user may be using the workstation at any given time. All users are counted individually toward the total clients allowed by the license.
- Q-24** Can a person have multiple BioPassword templates that would allow access to different workstations?
- A-24** Yes. Just as the network operating system permits a single user to have multiple user accounts (user name and password), BioPassword seamlessly adds a layer of protection to each user account that an individual may have. For example, if an employee needs to access your organization's primary LAN and needs to access financial information on a separate domain, BioPassword will authenticate each domain account. Each BioPassword used is treated as a separate seat license for a specific account regardless of the domain.
- Q-25** If I biometrically enroll on my workstation, can I go to someone else's workstation and biometrically log in?
- A-25** Yes. BioPassword supports roaming between workstations that belong to the same domain.