



OMNI IDENTITY

BioPassword Enterprise Edition

## BioPassword Enterprise Edition

*Provided by Omni Identity, Inc.*

**BioPassword Enterprise Edition** *Biometric multi-factor authentication software solution based on the science of keystroke dynamics that protects user authentication by strengthening Active Directory password-based authentication for corporate networks and Citrix environments.*

**BioPassword Enterprise Edition** combats fraud, stolen information assets and identity theft problems associated with using traditional password security, such as internal security breaches, social engineering, password-cracking programs, and employee password sharing. BioPassword targets these problems by layering our proven biometric software technology with your existing Windows password environment to provide multi-factor authentication monitoring and enforcement using the most widely understood user authentication tool—the password.

### **Convenience**

With BioPassword Enterprise Edition, multi-factor authentication monitoring or enforcement can be deployed in your environment in a matter of hours giving enterprises the opportunity to monitor authentication activity and secure critical information assets. BioPassword conveniently integrates with existing Active Directory and Domain Controllers without requiring additional hardware or extra software. Enterprise Edition minimizes user administration and requires no change in user behavior.

### **Coverage**

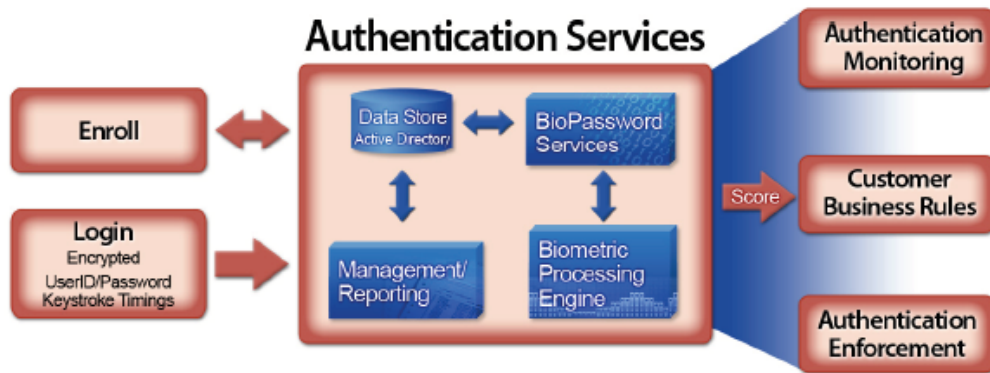
BioPassword Enterprise Edition is specifically designed for Windows and Citrix Presentation Server environments to protect Active Directory user accounts and provide complete multi-factor authentication coverage for your entire organization's corporate network and remote access needs. BioPassword leverages benefits provided by Active Directory's distributed authentication architecture making Enterprise Edition robust and scalable.

### **Cost**

BioPassword Enterprise Edition delivers multi-factor authentication to your users for less than one third the cost of tokens and smart cards. BioPassword reduces the burden on IT help desks by eliminating the need for short password reset cycles and password complexity requirements. The total cost of ownership (TCO) is extremely low since there is nothing that can be lost or stolen and ongoing management is minimal.

### **BioPassword Enterprise Edition at Work**

BioPassword permits network users to gain access to resources only after being authenticated by two-factor identification. This method goes well beyond standard password usage, by delivering secure and reliable user authentication (usually referred to as strong user authentication). BioPassword uses two methods (or factors) to accurately identify individuals before granting them access to corporate information and resources. First, the user must know both the correct user name and password and second, the user's typing rhythm must match the biometric template that has been stored and secured by the system.



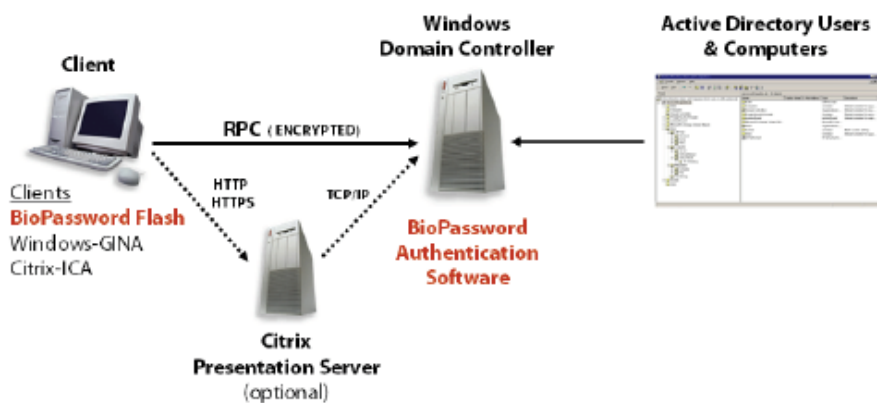
Basic Authentication Process:

- 1) User types a user name and password at his/her workstation.
- 2) BioPassword Client collects and sends the individual's typing sample in addition to the standard Windows logon process.
- 3) User is authenticated as an authorized user.
- 4) Windows Events are generated to enable audit trails, monitor authentication activity, and facilitate regulatory compliance.

## BioPassword Enterprise Edition

*BioPassword Enterprise is comprised of two primary components. BioPassword Enterprise Edition is installed on all Windows Domain Controllers and each workstation where strong authentication is required.*

*BioPassword administration leverages your existing approach to managing groups and users by extending the existing Microsoft Active Directory users and computers snap-in. BioPassword simply adds attributes to domain, user, and computer objects enabling an immediate and scalable deployment across your enterprise.*



## BIOPASSWORD COMPONENTS

BioPassword Enterprise Edition (BPE) Components:

- 1) BioPassword Enterprise Authentication Service – Exposes RPC interfaces for client components to create templates and authenticate users.
- 2) BioPassword Subauthentication DLL – Windows extension to domain controller login mechanism to verify and enforce biometric logon.
- 3) Windows Active Directory Users and Computers (ADUC) Extension – Uses the ADUC MMC to manage user and group settings for security levels and policy.
- 4) BioPassword Client (GINA) – Extends and does not replace the Windows Client Login UI (GINA) to moderate enrollment process and logon.
- 5) BioPassword Client Service – Captures keystroke timings for secondary authentication scenarios, for example:
  - a) Windows Change Password, RunAs and Join Domain dialogs
  - b) “Connect As” dialogs
  - c) Command line windows that are executing “Net use”
  - d) Command line windows that are executing “RunAs”

## **CITRIX INTEGRATION**

### **Citrix Presentation Servers**

BioPassword Clients can be installed on Citrix Presentation servers that require biometric security. BioPassword and GINA integration enforce biometric authentication for accessing published applications from a Citrix Presentation server. ICA sessions can be monitored and biometrically enforced by installing the BioPassword ICA Virtual Driver. Biometric authentication is achieved by installing both BioPassword Virtual Drivers and ICA Client.

### **Citrix Web Interface**

BioPassword protects external access to Citrix-published applications by integrating the Web Interface with the BioPassword Flash control to capture keystroke timings. Installation is a one-click execution of the BioPassword Web Interface installer.

### **Citrix ICA Clients**

ICA clients invoke the BioPassword virtual drivers to capture keystroke timings locally on clients and transmit them to the server through existing Citrix virtual channels.

### **Citrix STA (Secure Ticket Authority) server**

BioPassword STA installer runs on the Presentation Servers that are identified in the Secure Gateway configuration. STA supports the brokering of communication between the Secure Gateway server and the domain controller where BioPassword Service is installed.

## **BIOPASSWORD ADVANTAGES**

BioPassword has clear advantages over other authentication solutions including:

### **Usability**

- User-friendly - No change in user behavior.
- Non-invasive – Behavior based biometric, no capture of physical information like fingerprints, faces, or retina scans.
- Available anywhere there's a keyboard - No special equipment

### **Security**

- "Rhythm" cannot be shared, lost or forgotten.
- ONLY "resettable" biometric – Simply generate a new template.
- Authenticates the User - Not the browser settings, geo-coordinates, or pictures.

### **Integration**

- Seamlessly integrates with existing technology environments and processes.
- Scalable across the Enterprise and the Internet.

### **Cost**

- Reduced password changes results in fewer help desk calls and lower support costs.
- Strengthens password security, minimizing the benefits gained by increasing the complexity of user passwords.
- Does not require distribution, management or replacement of a special sensor, tokens, cards or keyboards.

By using BioPassword, the risk of easily guessed or weak passwords are irrelevant and stolen credentials completely worthless.

## **FEATURES AND BENEFITS**

### **Biometric Authentication Based on Keystrokes**

Accurately verifies user authentication through biometric science.

### **Software-Only Authentication**

Easy-to-use authentication software without any special hardware to install or maintain.

### **Enterprise-Wide Authentication Monitoring**

Utilizes Windows Event Logging to monitor and log all non-biometric and BioPassword logons.

### **Integration with Microsoft Active Directory (AD)**

Leverages existing Windows Active Directory environments to reduce complexity and increase scalability.

### **Integration with Citrix Presentation Server 3.0 and 4.0**

Adds two-factor authentication to Citrix internal and remote connectivity solutions.

### **Extends Biometric Authentication for Initial Logon and Secondary Authentication**

Supports initial Windows Logon and secondary authentication mechanisms such as Run As and Connect As.

### **Adaptive Biometric Learning**

Updates user's BioPassword template over time to increase security and usability.

### **Customizable Security Levels**

Manage BioPassword security levels user-by-user, or by Active Directory Groups to meet usability and security requirements.

### **Supports Windows Terminal Services Logon**

Meets enterprise connectivity needs with full support.

## ***Technical Specifications***

Supported Environments:

#### **Operating Systems**

- Windows 2003 Server
- Windows XP
- Windows 2000 Server
- Windows 2000 Professional

#### **Active Directory Domain Functional Levels:**

- Windows 2003 Native Mode
- Windows 2003 Mixed Mode
- Windows 2000 Native Mode

#### **Active Directory Forest Functional Levels:**

- Windows 2003
- Windows 2000

#### **BioPassword supports the following Citrix Components:**

- Presentation Server 3.0
- Presentation Server 4.0
- Citrix Web Interface 3.0
- Citrix Web Interface 4.0
- Citrix Web Interface 4.2
- Citrix Secure Gateway 2.0
- Citrix Secure Gateway 3.0

## **Omni Identity, Inc.**

499 North Canon Drive, 4<sup>th</sup> Floor  
Beverly Hills, CA 90210 USA

310-540-1115 | main

866-639-9840 | fax

[www.omniidentity.com](http://www.omniidentity.com)

[info@omniidentity.com](mailto:info@omniidentity.com)