Abstract: This White Paper describes how BioLink IDenium functions to 1) increase security in distributed enterprise-wide networks, 2) manage user account in various operating systems environments; 3] reduce overhead associated with password management and 4) increase user convenience and work-flow efficiency for enterprise networks. Product features are presented with diagrams and screenshots.
Copyright

The information contained in this document represents the current view of BioLink Solutions on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of BioLink Solutions, and BioLink Solutions cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. BIOLINK SOLUTIONS MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BioLink Solutions.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

©2011 BioLink Solutions. All rights reserved.

BioLink, IDenium, U-Match are either registered trademarks or trademarks of BioLink Solutions in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Contents

1. Introduction
   1.1 Password Management
   1.2 Biometric Innovations
   1.3 Distributed Networks

2. BioLink IDenium
   2.1 Architecture
   2.2 IDenium Server
   2.3 Core biometrics
   2.4 Scaling
      Replication
   2.5 Fault-tolerant features
      Multiple IDenium Servers
      Caches
   2.6 Encryption and data security

3. IDenium product family
   3.1 BioLink IDenium for Active Directory

4. IDenium for Active Directory
   4.1 IDenium for Active Directory architecture
   4.2 IDenium for Active Directory components
      Client-side applications
      Server-side applications
   4.3 IDenium for Active Directory installation guidelines
   4.4 IDenium for Active Directory system requirements
      Client Workstation Requirements
      Administrator Workstation Requirements
      Domain controller requirements
      Supported Devices

5. IDenium maintenance
   5.1 Logging
   5.2 Uninstallation
   5.3 Support and troubleshooting
Table of Figures

Figure 1. Sample distributed network ................................................................. 3
Figure 2. IDenium Authentication Environment .................................................. 4
Figure 3. The underlying mechanism of BioLink IDenium Microsoft Windows environment used as an example) ................................................................. 6
Figure 4. Network segment with only one IDenium Server ............................... 8
Figure 5. Network segment with more than one IDenium Server .................... 9
Figure 6. IDenium fault-tolerance ........................................................................ 10
Figure 7. IDenium for Active Directory operation mechanism ....................... 13
Figure 8. Geographically distributed corporate network with two domains ........................................................................................................... 15
Figure 9. The architecture of IDenium for Active Directory ............................ 15
1. Introduction

Logical access control to enterprise IT resources must include access and security methods that are appropriate for the policies set by each corporation or government agency.

Each organizational entity has its own set of corporate standards and rules and various operating system environments with an enormous number of user accounts granting access to the enterprise resources depending on the user roles and rights. Therefore, a common user with one or more accounts in different applications and operating environments will have to remember multiple, complex passwords, user names, obtain digital certificates or even produce a smart card simply to log on. All these routines lead to serious leaks in the entire company’s information security system that can both result in economic losses and compromise trade secrets.

These leaks appear because a password and user name can be forgotten, a digital certificate stolen or modified and hacked, a smart card given to another person, willingly or unwillingly, and all information stored on it erased or reprogrammed. All these dubious methods are the daily bread for those who wish to fake the identity of law-abiding citizens, sneak into protected premises, steal information resources and transmit it to competitors or other third-parties.

That is why password and identity management is now a major task for IT professionals.

1.1 Password Management

Password management can soak up precious financial and human resources from the IT department. Studies have shown that 1) password management can cost as much as $30 to $65 or more per user, per month (as high as $75 per help desk incident), and 2) 40% of help desk calls are password related. (Gartner Group)

In addition, users have a hard time remembering the complex and ever-changing passwords required to maintain a trusted security environment. By replacing or augmenting the traditional password method of access, password management costs can be reduced and an additional security layer can be provided without adding complexity for the user.

It is obvious for every company manager that securing information inside an enterprise environment is of special significance. That is why, when one talks about security and management, user experience and streamlined workflow, usability and cutting-edge brand new technologies, the subject relates to biometric solutions and innovations.

1.2 Biometric Innovations

Some time ago, the first sentence in this subject would describe biometrics as a technology, quoting various definitions and depicting features, all of which are purely theoretical and have nothing practical to offer.

Now, though, with biometric technologies and solutions conquering the world of IT and enterprise management, almost everyone has at least a
basic understanding of what biometrics does, what it is needed for, and how he (or she) can employ it to serve his or her own needs.

However, a new challenge has emerged - multi-biometrics, utilizing brand new technologies, cutting-edge mathematical ten-print algorithms, using a combination of various biometric features to identify one individual. In fact, multi-biometrics comprises fingerprint, iris, facial, voice, handwriting and other types of recognitions into one complete, universal solution that can be deployed both in small company and in large enterprise networks. Multi-biometrics introduces a new era in creating and maintaining biometric security systems, allowing flexible scalability, fault-tolerance, fast ROI and the highest security level ever achieved in corporate information systems. BioLink has already offered ten-fingerprints support in most of its products (including IDenium) and multi-biometric solutions are also on their way to potential customers (visit BioLink’s web-site www.biolinksolutions.com for more information on multi-biometrics).

The speed of biometric calculations has also been drastically increased, enabling the usage of biometrics even in international enterprises with branch establishments all other the world with highly distributed sophisticated network resources.

### 1.3 Distributed Networks

Nowadays the common network structure of an ordinary company is not as simple and straightforward as it was before. Distributed networks in large international enterprises can be the most sophisticated establishments, which are hard to visualize and comprehend.

In addition, the amount of money being spent on enterprise network management has drastically increased in recent years. With the vast expansion of Internet-related technologies, the problem of information security in distributed systems again tops the list of tasks facing IT personnel. More and more resources are still required to maintain invulnerable corporate networks, which are resistant to external hacking attacks.

For example, a company network may include the following:

- Standard Windows local network with Active Directory;
- Remote (or web) servers, web-consoles and other custom applications demanding user authentication for their access (or launch);
- Remote desktops (Citrix, Windows Terminal, etc.);

Such a network is depicted on the figure below. The sample network there is visually divided into four segments, each demanding dedicated user authentication.
In spite of the ability to authenticate a user by means of his (or her) Windows account, the user is most likely to have an enormous number of different accounts, each of them linked to a specific operating system and/or environment. This will result in a so-called “password overload”, for the user will have to remember all these user names and passwords to all accounts he or she uses in the business process.

Despite all the common attempts of security IT personnel to strengthen all lines of defense (using fundamentally changing passwords and employing such other means of user identification as smart cards, digital certificates, PINs etc), the network still has vulnerabilities due to the human factor. Perhaps the severest and the most unavoidable vulnerability is that a user has to remember multiple passwords (or possess other means of self-identification).

BioLink IDenium is targeted to relieve users of passwords and other authorization tools. After IDenium installation, all they need is to log on to any operating environment or resource and to place one of their ten fingers on the biometric scanner. IDenium allows the IT professional to concentrate on other important tasks, and not waste time changing passwords on a daily basis for forgetful users.

The figure below depicts the distributed enterprise network after IDenium has been deployed.

**Figure 1. Sample distributed network**
The scheme on Figure 2 shows that all user authentication procedures are now controlled by IDenium software. IDenium manages all information about different user accounts and user credentials valid for these accounts.

A user will not have to remember user names or passwords, or carry smart cards. A user can put aside all internal authentication methods and concentrate on his or her direct business processes.
2. BioLink IDenium

BioLink IDenium is a biometric authentication system, which will significantly enhance your operating environment security mechanisms (incorporating user names and passwords) by applying one of the most reliable and efficient user recognition solutions - fingerprint recognition. This will improve fail-safe secured access to various application resources, reinforce protection of confidential information, and streamline user experience and workflow.

2.1 Architecture

If a company uses several operating environments, network configurations, and password protected applications (see Figure 1 for an example), its employees are obliged to have dozens of user accounts and memorize their numerous names and passwords. All these accounts can be in fact linked to just one individual. IDenium means all the account information pertaining to one user, an IDenium user, can be brought together in a single database.

The underlying mechanism of BioLink IDenium architecture is the centralized storage of different user accounts in one repository, easily accessible for all applications that execute user authentication tasks. BioLink IDenium stores user credentials (e.g. passwords, logins, etc.) and retrieves them after the presentation of biometric identifiers (fingerprints).

If the presented biometric identifiers match with the stored ones, the appropriate user account data (user name (login) and password) are sent to the application requesting them. Now it is up to the application to decide how the acquired user credentials will be processed. Whether or not the user is allowed to perform the desired action (logon to a computer, access protected resources, etc.) depends entirely on the current application’s access rules. IDenium has nothing to do with such rules. The task of IDenium is only to return valid user credentials for the given biometric identifiers.
Consider Figure 3. First of all **the synchronization** of biometric credentials is made between the IDenium storage and the IDenium server (0). The **IDenium storage** stores IDenium–related policies and biometric identifiers. The **IDenium server** performs matching operations.

A user supplies his or her credentials at the request of a custom application. Instead of typing a user name or password, he or she places a fingerprint on the biometric scanner. Then the acquired biometric identifiers are sent to the IDenium server using a special Queue. More technically, the client application initializes a request for identification (which includes biometric identifiers) and puts it into the Queue (1). The IDenium server constantly peeks the requests for identification, processes them and returns the identification results (2) (if the match was found the results contain user credentials). The application, which originated the request, waits for the identification results. As soon as results become available the application dequeues the results to obtain the user credentials.

The custom application sends the acquired user credentials to the domain controller to perform authentication (3). According to the authentication results, the custom application decides whether to execute the desired action or not.

As a part of the IDenium system, BioLink offers the following components, which substitute the “custom application” concept in the preceding example:

- **BioLink IDenium Windows Client** is responsible for logging on to Windows workstations, applications and resources.
- **BioLink Citrix Logon** manages access to Citrix remote desktops.
• **BioLink Terminal Services Components** is responsible for logging on to Windows terminal servers and resources.

It is possible to enable IDenium support for any custom application using **IDenium SDK** (if you need more information about IDenium SDK and other IDenium-related products, please visit our web-site at [www.biolinksolutions.com](http://www.biolinksolutions.com)).

Let’s return to **Figure 2. IDenium Authentication Environment** on p. 4. As you can see, IDenium stores information about all user accounts (Windows, Citrix and custom applications accounts). As a result, when a user presents his or her biometric identifiers, they do not need to bother about user names, passwords, accounts, etc. They simply place a fingerprint on the biometric scanner and proceed with their business tasks.

All these outstanding features are brought to life by the **IDenium Server**.

### 2.2 IDenium Server

The **IDenium Server** processes client requests as well as generates reply packages containing user identification details.

The main IDenium Server features are:

- **Ease of deployment** - can be deployed on any Windows workstation.
- **Ease of installation** – to bring the IDenium Server into operation, just install it on any computer in your domain network.
- **Ease of scaling** – you can install as many server instances as you need to improve your network’s performance and enable fault-tolerance.
- **Zero administration** – once installed, the IDenium Server requires NO user management or intervention in order to continue normal operation.

However, the IDenium Server could be just a simple matching device without cutting-edge BioLink biometrics.

### 2.3 Core biometrics

Cutting-edge mathematical biometrical algorithms constitute the core of the BioLink IDenium system.

The biometric part of the system provides two principle functions:

- **Reading the fingerprint and its transformation into digital form.** The digital image is stored on the IDenium Server as a template. The fingerprint image itself cannot be restored using the template.
- **User identification.** To identify the user the scanned image is compared with the existing template.

User fingerprints should be enrolled in IDenium to enable biometric user identification. Up to ten fingerprints may be enrolled for each IDenium user. For each of the enrolled fingers a digital template is created, providing immense security and the inability to recreate the original fingerprint image from the template. This template, along with other IDenium-specific user data, is stored on the IDenium Server and is being used then (custom) applications require user authorization to complete a required operation.
2.4 Scaling

Scalability is a great feature of IDenium and, in particular, of the IDenium Server.

If your company is small or you are planning phased deployment (for example, you are deploying an IDenium system for testing purposes in just the IT department), you only need to acquire one IDenium Server and it is easy to try the system in action.

You can be sure that if you decide to expand the IDenium network for the entire enterprise network, you only need to purchase the number of IDenium Servers that are required.

Moreover the expansion may be required if you implement a number of custom applications that generate many more user authentication requests than previously. In this or other cases (for example, under a drastic increase of user workstations in the network, company expansion, branch office establishment and so on) the speed of requests processing may be severely affected. The solution to this problem is simple: purchase and deploy as many IDenium Servers as needed to augment corporate network bandwidth and increase the overall speed of user authentication requests processing.

![Diagram of a network segment with only one IDenium Server](image)

**Figure 4. Network segment with only one IDenium Server**

It is possible to install as many IDenium Server instances as your network requires. Each additional instance of an IDeniumServer drastically increases the speed of matching operations and user logon procedures.
As you can see on the figure above, all requests from user workstations are processed by IDenium Servers in random order.

**Replication**

If you have more than one IDenium Server in your local network, all IDenium-specific data (user accounts, credentials, biometrics, etc) will be automatically replicated (using build-in Active Directory mechanism) between all IDenium Servers.

### 2.5 Fault-tolerant features

BioLink IDenium is a completely fault-tolerant solution. This is achieved by installing multiple IDenium Servers in the network (see *Scaling* on p.8 for more information).

**Multiple IDenium Servers**

To enable fault-tolerance you need at least two IDenium Servers.

Data synchronization between IDenium Servers is performed automatically.
Caches

Another way of creating a fault-tolerant IDenium network is to use caches.

The IDenium caches work in the following way: after the user work session is successfully established, user confidential data (user names and passwords, biometric identifiers, etc) are placed in a cache on the local hard disk. When the IDenium server becomes unavailable, the user credentials, stored in the cache on the user's local computer, are used to access the protected resources.

Therefore, this way is not recommended as it places your system security at lower levels.

2.6 Encryption and data security

To ensure that no one can intercept and decipher biometric data, IDenium uses combination of SSL(AES128) and Active Directory access rights. These algorithms provide a reliable level of security, which seamlessly integrates with other encryption techniques, employed in the targeted network.

The encryption is enabled throughout the course of data exchange with the IDenium Server. This ensures that data in all channels that transfer biometric identifiers can not be intercepted, deciphered or in any way compromised.

In addition, all biometric data is stored in the IDenium storage not in raw images/data, but in specially encrypted digital templates (or models). It is
impossible to restore an original fingerprint from these templates. Such a feature makes the task of deciphering IDenium data the most complicated possible and almost impossible to complete.
3. IDenium product family

The IDenium system comprises various software products tailored for specific business purposes, unified by the BioLink biometric core, which employs BioLink’s cutting-edge mathematical algorithms and advanced biometric technologies.

The BioLink IDenium product family includes the following:

- BioLink IDenium for Active Directory;
- BioLink IDenium Standard Edition;
- BioLink IDenium Enterprise Edition;
- BioLink IDenium Local Edition.

3.1 BioLink IDenium for Active Directory

If distributed enterprise-scale networks are used, it is recommended to use BioLink IDenium for Active Directory.
4. IDenium for Active Directory

Almost every company with a Windows network environment employs Active Directory as a directory service. Active Directory allows the central management of resources in a geographically distributed corporate network.

To place information security on a new level in such networks, BioLink has introduced the **IDenium for Active Directory** solution.

The following sections focus on a description of BioLink IDenium in Windows Active Directory networks.

4.1 IDenium for Active Directory architecture

IDenium for Active Directory is tailored to significantly enhance security mechanisms provided by a Microsoft Windows operating system.

The BioLink IDenium for Active Directory is focused on achieving the following goals, compared with Standard and Enterprise editions:

- **Fault-tolerance enhancement** (by allowing Active Directory to store all IDenium data (including IDenium policies and biometric identifiers));
- **User authentication in geographically-distributed enterprise networks**, using Active Directory data replication mechanisms;
- **Easier, Windows-native, user-friendly** administration of user accounts and biometric data.

![Figure 7. IDenium for Active Directory operation mechanism](image-url)
Consider the Figure above. It is almost the same as discussed in the IDenium architecture section on p.6. The only difference is that Active Directory substitutes the IDenium storage concept. In addition, all queues created by server(s) are also controlled by AD thus eliminating the need for installation of other components.

As you have already learned, the principle underlying the IDenium mechanism is that different devices, which can translate a variety of biometric characteristics of an individual into digital form, are attached to the user workstation and are employed as one of the main sources of information about who is actually trying to gain access to various information resources. A user places their finger on the scanner, the server matches their fingerprints with the stored ones and returns the identification result.

The IDenium for Active Directory working mechanism can be described in the following way:

1. When a user begins a logon to a Windows workstation, they place a finger on the fingerprint scanner.
2. The user workstation generates a request for identification (which includes digitally encrypted fingerprint image – i.e. fingerprint template) and places it in the queue in AD.
3. The IDenium server peeks the queue for identification requests, processes them and returns the identification results (if a match proves successful, the server returns the user credentials ((user name (login) and password)).
4. The workstation which originated the request for identification acquires user credentials and sends the credentials on the domain controller to perform user authentication
5. As a result the user gains access to the application’s resources, according to the user access rights and group policy rules.

The paragraphs below describe the architecture of IDenium for Active Directory in a more sophisticated environment, in particular, when a network consists of two (or more) possibly geographically distributed domains (see figure below).
IDenium seamlessly integrates with such a configuration, allowing for the user registered in domain 1 (DC1 on the figure above) to log on easily to a computer located in domain 2 (DC2) by applying a fingerprint.

Consider the figure below which combines the IDenium operation mechanism (see Figure 7 IDenium for Active Directory operation mechanism) with the geographically distributed approach (see Figure 8 Geographically distributed corporate network with two domains).

**Figure 8. Geographically distributed corporate network with two domains**

**Figure 9. The architecture of IDenium for Active Directory**

Keys to abbreviations:
- WS1 – workstation in domain 1.
• IS1 – IDenium server in domain 1.
• DC1 – domain controller 1.
• ROOT DC – root domain controller, containing the GC (Global catalog).
• ADD – Active Directory Database.
• WS2, – workstation in domain 2.
• IS2 – IDenium server in domain 2.
• DC2 – domain controller 2.
• WS-Admin – local administrator workstation.

Commentaries:
• The local network administrator (WS-Admin) can control all user accounts in the network. Using Active Directory, the administrator can manage all objects in the Active Directory distributed structure, including user accounts. The administrator is able to allow or restrict fingerprint authentication for a specific user account or user group.

4.2 IDenium for Active Directory components

BioLink IDenium for Active Directory is a distributed system involving components that are installed on servers and client workstations.

Client-side applications

The client part of the IDenium software consists of the following components:

• **BioLink IDenium Windows Logon** (responsible for user authentication at system log on)

• **BioLink IDenium Admin Pack** (tailored for system administrators, allowing them to centrally manage a users’ biometric credentials, configure user workstations and perform other IDenium administrative tasks).

Server-side applications

The server IDenium software includes the following components:

• **BioLink Password Synchronizer** is designed to provide means of user credentials synchronization between Active directory database and BioLink IDenium server(s));

• **BioLink IDenium Server** (constitutes the core of the biometric security system; its functions include processing of client requests as well as generating reply packages containing user identification details. The main parameter associated with the server is the superior level of security it provides for its own data and the high speed of processing of concurrently received queries).

4.3 IDenium for Active Directory installation guidelines

BioLink IDenium for Active Directory deployment is not as complicated as it may seem. First, local IT infrastructure should be constructed and the network established and configured. It is also recommended that you create all group policies and define access rights; in other words, plan
your local distributed network thoroughly. Obviously, you should make certain that everything is functioning as you have planned.

Only then should you start deploying IDenium.

IDenium for Active Directory components should be installed in the following order:

1. **Step 1: Extending the Active Directory Scheme.** At this step, the IDenium components and attributes are added and registered in the Active Directory scheme.

2. **Step 2: Installing Password Synchronizer component.** At this step you should install the Password Synchronizer component on every domain controller in your network.

3. **Step 3: Installing and deploying BioLink IDenium server.** At this step you should install and deploy BioLink IDenium server on any computer you like in your network.

4. **Step 4: Installing Admin Pack.** It is installed on the network workstation dedicated for executing administrative tasks.

5. **Step 5: Installing BioLink IDenium Windows Logon on user workstations.** BioLink IDenium Windows Logon is responsible for user biometric authentication at logon to the operating system, domain or computer resources.

### 4.4 IDenium for Active Directory system requirements

System requirements fall into four major categories, including:

- **Client workstation requirements** (all end-user computers should meet these requirements. In addition, each end-user workstation should be equipped with a biometric scanner).

- **Administrator workstation requirements** (an administrator workstation may be a local administrator computer or a dedicated computer, intentionally tailored for performing IDenium administrative tasks. If the administrator has the right to enroll a user’s fingerprints, a biometric scanner should also be attached).

- **Domain controllers requirements** (it is strongly recommended that all your domain controllers should meet these requirements).

- **Supported biometric devices.**

**Client Workstation Requirements**

- Microsoft Windows 2000 (Service Pack 4), XP, 2003 Server SP2, Vista
- Personal computer with a CPU Pentium 200 MHz or higher
- 64 MB of RAM (132 MB recommended)
- 40 MB of free hard disk space
- CD-ROM drive (necessary for installation)
- Free USB port for the USB BioLink U-Match Mouse or MatchBook.
Administrator Workstation Requirements

- Microsoft Windows Server 2000 (Service Pack 4), 2003 (Service Pack 2) , XP with the Active Directory management console installed
- Personal computer with a CPU Pentium IV 1500 MHz or higher
- At least 512 MB RAM
- 200 MB of free hard disk space
- CD-ROM drive (necessary for installation)
- Free USB port for the USB BioLink U-Match Mouse or MatchBook

Domain controller requirements

- Microsoft Windows Server 2000  (Service Pack 4), 2003  (Service Pack 2)
- Personal computer with a CPU Pentium IV 1500 MHz or higher
- At least 512 MB RAM
- 200 MB of free hard disk space

Supported Devices

The following devices are supported:

- USB BioLink U-Match Mouse
- BioLink U-Match MatchBook.
- BioLink U-Match MatchBook 3.0.
- BioLink U-Match MatchBook 3.5.
- UPEK scanner
5. IDenium maintenance

IDenium is a user-friendly solution and does not require any sophisticated skills, long-term IDenium experience or extra training. All administrative tasks can be executed using the standard interface of the host operating system (for example, IDenium administration in Windows Active Directory environment is performed by means of an Active Directory User and Computer snap-in).

5.1 Logging

IDenium has a built-in logger, which provides administrator-friendly access to all events that occur within the IDenium system. These events comprise the following:

- User creation;
- Biometric identifier enrollment;
- User authentication and access to the targeted operating system;
- Synchronization of user account and other IDenium-related data

The IDenium log can be viewed using a standard Computer Management console. The logger enables monitoring of the IDenium system health status, locating, tracing and eliminating errors, obtaining supplemental information about IDenium operations and performing other IDenium maintenance tasks.

5.2 Uninstallation

IDenium software can be completely uninstalled if you wish to revert to your previous configuration. It is assumed that IDenium client components should be uninstalled first; only then can the IDenium server software be removed.

However, it is impossible to delete IDenium objects from the Microsoft Active Directory schema, because the process of Active Directory extension is irreversible. The only way to return to the previous Active Directory schema is to restore the Active Directory schema from back-up (although losing all changes made after the date, when the back-up was created).

5.3 Support and troubleshooting

If you have any questions, the BioLink Technical Support Department team can be contacted at support@biolinlsolutions.com