Abstract: This White Paper describes how 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.
Contents

1. Introduction ........................................................................................................................................ 1
   1.1 Password Management .................................................................................................................. 1
   1.2 Biometric Innovations ............................................................................................................... 1
   1.3 Distributed Networks ............................................................................................................... 2
2. IDenium .................................................................................................................................................. 5
   2.1 Architecture .................................................................................................................................. 5
   2.2 IDenium Server ............................................................................................................................. 5
   2.3 Core biometrics ............................................................................................................................. 6
   2.4 Scaling ......................................................................................................................................... 6
   2.5 Fault-tolerant features ............................................................................................................... 8
   2.6 Encryption and data security ....................................................................................................... 9
3. IDenium Product Family ....................................................................................................................... 9
4. IDenium Local Edition .......................................................................................................................... 9
5. IDenium Enterprise Edition .................................................................................................................. 9
   5.1 IDenium for Enterprise Edition Architecture ............................................................................. 10
   5.2 Integration with Active Directory ............................................................................................... 12
   5.3 IDenium Enterprise Edition Components .................................................................................. 13
   5.4 IDenium Enterprise Edition installation guidelines ..................................................................... 13
   5.5 IDenium Enterprise Edition System Requirements ..................................................................... 14
6. IDenium Maintenance ........................................................................................................................... 15
   6.1 Logging ....................................................................................................................................... 15
   6.2 Uninstallation ............................................................................................................................... 16
   6.3 Support and Troubleshooting ..................................................................................................... 16
7. Where to Find Additional Information ............................................................................................... 16
1. Introduction

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

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

These leaks largely appear due users forgetting passwords or user names, digital certificates being stolen, modified, or hacked, and smart cards given to another person willingly or unwillingly, with all information stored on it erased or reprogrammed. These are the usual methods for identity thieves and hackers that routinely co-opt the identity of legitimate users in order to enter into protected premises, steal information, and transmit it to either competitors or other third-parties.

This is why password and identity management is one of the major tasks of IT professionals.

1.1 Password Management

Password management takes away 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 it is possible to reduce password management costs and provide an additional security layer without adding complexity for the user.

It is obvious for every company manager that the task of securing information inside an enterprise environment is of extreme importance. Which is why, when one talks about security and management, user experience and streamlined workflow, usability and cutting-edge brand new technologies, invariably the conversation will lead to biometric solutions.

1.2 Biometric Innovations

Some time ago, a first sentence in this topic 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 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 they can employ it to serve their own needs.

However, new challenges have 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 can comprise fingerprint, iris, facial, voice, handwriting and other types of recognitions into one complete universal, solution that can be deployed for networks in both small and large companies and as well as in the enterprise. 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 the 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 the potential customers.

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

1.3 Distributed Networks

A common network structure of an ordinary company is not as simple and straightforward as it had been before. Distributed networks in large international enterprises can be the very sophisticated, which makes it hard to visualize and comprehend.

In addition, the amount of money being spent for the management of enterprise networks has drastically increased in recent years. With the vast expansion of Internet-related technologies the problem of information security in distributed systems has once more come to the forefront IT personnel’s tasks. More and more resources are still required to secure vulnerable corporate networks against persistent attacks.

For example, a company network may include the following:

- Standard Windows Network using Active Directory
- Remote (or web) servers, web-consoles and other custom applications demanding user authentication to access (or launch) them
- Remote desktops (Citrix, Windows Terminal Services, etc.)

Such a network is depicted on a figure below. The sample network there is visually divided into four segments, each of them demanding dedicated user authentication.
In spite of a user authenticating via normal means (i.e. their Windows account) most users will have an enormous number of different accounts with each of them linking to a specific operating system or networking environment. This will result in a “password overload” since the user will have to remember all of these separate user names and passwords to all accounts they need to use throughout their day.

Despite common attempts of security IT personnel to strengthen all lines of defenses (using strong changing passwords, employing other means of user identification – smart cards, digital certificates, PINs, etc.), networks still have vulnerabilities due to human factors. The most prominent of which is that a user has to remember multiple passwords (or possess other means of self-identification).

IDenium minimizes the use of passwords and other authorization tools. After IDenium’s installation, all users would need to log on to any operating environment, or resource, is to place one of their ten fingerprints on a biometric scanner. IDenium allows IT professionals to concentrate on other important tasks, instead changing passwords for forgetful users.

The figure below depicts the distributed enterprise network after IDenium has been deployed.
The scheme on figure 2 shows all user authentication procedures are now being 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, passwords, or carry smart cards. They will not have to worry about all the different internal authentication methods previously used and can concentrate on their work.
2. IDenium

IDenium is a comprehensive biometric identification solution designed to manage access to corporate information resources of an enterprise-wide network. This solution is designed to handle identification issues of any organization using a Window Active Directory-based network.

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 numerous usernames and passwords. All these accounts can be instead linked to just one individual using a single account. IDenium brings together all account information pertaining to a user into a single database.

The underlying mechanism of IDenium’s architecture is the centralized storage of different user accounts in one repository, which makes it easily accessible for all applications executing user authentication tasks. 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 then sent to the application requesting them. Once presented, the application will proceed accordingly. Whether or not the user will be allowed access (logon to a computer, access the protected resources, etc.) depends on the application’s access rules. IDenium’s task is to return valid user credentials for presented biometric identifiers.

As a part of the IDenium system, the following components substitute the “custom application” idea in the preceding example:

- **IDenium Windows Logon** is responsible for the logon to the Windows workstations and resources.
- **IDenium Citrix Logon** manages access to Citrix remote desktops.

It is possible to enable IDenium support for any custom application via the **IDenium SDK**.

Returning to Figure 2. **IDenium Authentication Environment** on p. 4. 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 with user names, passwords, accounts, etc. They simply place a fingerprint on the biometric scanner and then continue with their work. This biometric credential storage and comparison is the primary responsibility of 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 features of IDenium Server are:

- **Ease of Deployment** – Can be deployed on any Windows system.
- **Ease of Installation** – It can be installed on any computer in your network.
- **Ease of Scaling** – Multiple can be installed as needed to improve network performance and to enable fault-tolerance.
- **Zero Administration** – Once installed, IDenium Server requires NO user management or intervention in order to continue normal operation.

### 2.3 Core Biometrics

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

The biometric part of the system provides two principle functions:

- Reading the fingerprint and transforming it into digital form. The digital image is then 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 the IDenium to enable biometric user identification. It is possible to enroll up to ten fingerprints for each IDenium user. For each of the enrolled fingers, a digital template is being 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 then used by (custom) applications that require user authorization to operate.

### 2.4 Scaling

Scalability is one of IDenium’s greatest strengths.

With smaller firms or for planning a large, phased deployment (for example, deploying IDenium for testing purposes in an IT lab environment), it is best to evaluate one IDenium Server too see the system in action.

Moreover AD expansion may be possibly required if there are a number of custom applications that generate more user authentication requests. In this, or other cases (for example, drastic increase of user workstations in the network, company expansion, branch offices establishment) the speed of processing login requests may degrade as the user and workstation count increase. With IDenium, the solution to this problem is simple: More IDenium Servers can be deployed as needed to augment corporate network bandwidth and to increase the overall velocity of user authentication requests processing.
There is no upper limit as to the amount of IDenium Server instances which can be deployed to serve your network’s needs. Each additional instance of IDenium Server drastically increases the speed of matching operations and improves the velocity of the user logon procedures.

As you see on the figure above, all requests from user workstations are being processed by IDenium Servers in random order.
Replication

IDenium Server caches user accounts from the Active Directory database. 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 between IDenium Servers by means of standard Active Directory mechanisms.

2.5 Fault-tolerant features

IDenium is a fault-tolerant solution. This is achieved by means of installing multiple IDenium Servers in the network (see Scaling topic on for more information).

Multiple IDenium Servers

To enable fault-tolerance there needs to be at least two IDenium Servers.

Data synchronization between IDenium Servers is performed automatically.

Caches

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

IDenium caches work in the following way: After a user’s work session is successfully established, the user’s confidential data (user name, passwords, Password Vault scripts, etc.) are placed in a cache on the local hard disk. When an IDenium server is not available the user credentials, stored in the cache on the user’s local computer, is used to access to protected resources.
However, this is not a recommended configuration since it lowers the security of your workstation. This configuration should only be used when appropriate and the benefits outweigh the risks of deployment in this manner.

2.6 Encryption and data security

To ensure no one can intercept and decipher biometric data, IDenium uses strong symmetric and asymmetric algorithms (AES 128, for instance). These algorithms provide a reliable level of security, and seamlessly integrates with other encryption techniques employed in the target network.

Encryption is enabled all the time during interaction with IDenium Server. This ensures that data in all channels transferring biometric identifiers can not be intercepted, deciphered, or be in someway compromised.

In addition, all biometric data is stored on the IDenium Server not in raw images/data, but in specially encrypted digital templates (or models). It is impossible to restore an original fingerprint image from these templates.

3. IDenium Product Family

The IDenium system is comprised of 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 IDenium product family includes the following:

- **IDenium Local Edition**
- **IDenium Enterprise Edition**

4. IDenium Local Edition

IDenium Local Edition is a version of IDenium designed to work as a stand-alone version on systems that are not part of a domain or are not usually connected to a network.

The functionality of IDenium Local Edition is similar to the Enterprise Edition with the exception of integration with Active Directory.

For more information on this version, please contact your local authorized reseller.

5. IDenium Enterprise Edition

Almost every company with a Windows network environment employs Active Directory as a directory service. Active Directory allows companies to centrally manage resources in geographically distributed corporate network.
To place information security on a new level in such networks, BioLink introduced **IDenium Enterprise Edition** solution.

The next chapters focus on description of IDenium in Windows Active Directory networks.

### 5.1 IDenium for Enterprise Edition Architecture

IDenium Enterprise Edition is tailored to significantly enhance security mechanisms provided by Microsoft Windows operating system.

IDenium Enterprise Edition is focused on achieving the following goals in comparison with IDenium Local Edition:

- 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 6. IDenium Enterprise Edition operation mechanism](image)

Consider the figure above. It is almost the same as discussed in the IDenium architecture section. The only difference is that **Active Directory substitutes the IDenium storage** concept.

The principle underlying the IDenium mechanism is that different devices 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 and then the server matches their fingerprints with the stored ones and returns the identification result.

IDenium Enterprise Edition workflow can be described in the following way:
1. When a user begins a logon to the Windows workstation, they place their fingerprint 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 matches the acquired fingerprint image with stored one, and if there is a successful match, returns the user credentials (user name (login) and password) to the application requesting them.
4. The workstation that originated the request for identification acquires the user’s credentials and sends them to the domain controller to perform user authentication.
5. As a result, the user gains access to the application’s resources according to the user’s access rights and group policy rules.

The paragraphs below describe the architecture of IDenium Enterprise Edition in more sophisticated environment, in particular, when network consists of two (or more) possibly geographically distributed domains (see figure below).

![Figure 7. Geographically distributed corporate network with two domains](image)

IDenium seamlessly integrates with such a configuration allowing for user registered in domain 1 (DC1 abbreviation on the figure above) easily to log on to a computer located in domain 2 (DC2) by applying a fingerprint.

Consider the figure below, which combines IDenium’s operation mechanism (see Figure 6 IDenium Enterprise Edition operation mechanism) with the geographically distributed approach (see Figure 7 Geographically distributed corporate network with two domains).
Figure 8. The architecture of IDenium Enterprise Edition

Keys to abbreviations:

- WS1 – a 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 – a workstation in domain 2.
- IS2 – IDenium server in domain 2.
- DC2 – domain controller 2.
- WS-Admin – local administrator workstation.

Comments:

The local network administrator (WS-Admin) can control all user accounts on each IDenium server deployed in the local network. By means of Active Directory the administrator can manage all objects in the Active Directory distributed structure including user accounts. The administrator has the possibility to allow or restrict fingerprint authentication for specific user account or user group.

5.2 Integration with Active Directory

IDenium is fully integrated into Microsoft Active Directory and provides centralized management of user’s credentials & access rights, as well as easy installation of client components via AD group policies.

After installation, IDenium management tabs will be added in the standard Microsoft Management Console allowing IT managers and administrators to manage user accounts, their rights and privileges, register new users, and enroll biometric credentials right from Active Directory Users and Computers (ADUC).
Active Directory provides centralized storage, protection and transfer of a user's credentials.

User's rights and privileges management is also centralized and carried out by using the standard Active Directory Users and Computers (ADUC) Microsoft Management Console (MMC) snap-in.

The administrator defines and modifies the policy of user access to protected information resources allowing or denying biometric identifiers, passwords or smart-cards to be used for authorization.

The password synchronizer constantly and automatically monitors the accounts stored in the AD global catalog, and if necessary, updates the users credentials which the IDenium application server requires for identification.

5.3 IDenium Enterprise Edition Components

IDenium Enterprise Edition is a distributed system involving components that installed on servers and on the client workstations.

Client-side applications

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

- **IDenium Windows Logon** - responsible for user authentication at the system log on
- **IDenium Admin Pack** - tailored for system administrators allowing them to centrally manage users’ biometric credentials, configure user workstations and perform other IDenium administrative tasks.

Server-side applications

The IDenium server side software includes the following components:

- **IDenium Password Synchronization** - is designed to provide means of user credential synchronization between Active Directory database and IDenium Server(s)
- **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 characteristic 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.

5.4 IDenium Enterprise Edition Installation Guidelines

IDenium Enterprise Edition deployment is simple. First, local IT infrastructure should be constructed and network established and configured. It is also recommended that all group policies be created and access rights defined, in other words, plan your local distributed network thoroughly.

Once all infrastructure is in place and the network is running, then IDenium installation can proceed

IDenium Enterprise Edition components should be installed in the following order:
1. **Step 1: Extending the Active Directory Schema:** At this step, IDenium components and attributes are added and registered in the Active Directory scheme.

2. **Step 2: Installing Password Synchronization Component:** The Password Synchronization component needs to be installed on every domain controller in the network.

3. **Step 3: Installing and Deploying BioLink IDenium server:** IDenium server needs to be deployed on a server or workstation in the network.

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

5. **Step 5: Installing IDenium Windows Logon on user workstations:** IDenium Windows Logon is responsible for user biometric authentication at logon on workstation operating systems (clients) or other computer resources.

### 5.5 IDenium Enterprise Edition 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 (administrator workstation may be a local administrator computer or a dedicated computer intentionally tailored for performing IDenium administrative tasks. If the administrator will have the right to enroll user’s fingerprints, a biometric scanner should also be attached).
- Domain controller 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, Microsoft Windows Vista/7/8
- Personal computer with a CPU Pentium 1500 MHz or higher
- 256 MB of RAM (512 MB recommended)
- 200 MB of free hard disk space
- CD-ROM drive (necessary for installation)
- Network adapter
- Free USB port for the USB BioLink U-Match or i-Match.

#### Administrator Workstation Requirements

- Microsoft Windows 2000 (Service Pack 4), XP, 2003, Microsoft Windows Vista/7/8 with the Active Directory management console installed
- Personal computer with a CPU Pentium 1500 MHz or higher
- 256 MB of RAM (512 MB recommended)
- 200 MB of free hard disk space
- CD-ROM drive (necessary for installation)
• Network adapter
• Free USB port for the USB BioLink U-Match or i-Match.

**Domain Controller Requirements**
• Microsoft Server 2000 (Service Pack 4), 2003 (Service Pack 2), 2008/2012
• Personal computer with a CPU Pentium 3000 MHz or higher
• At least 512 MB of RAM
• 200 MB of free hard disk space

**IDenium Server Requirements**
• Microsoft Server 2000 (Service Pack 4), 2003 (Service Pack 2), 2008/2012
• Personal computer with a CPU Pentium IV 3000 MHz or higher
• At least 512 MB RAM
• 200 MB of free hard disk space

**Supported Devices**
• The following devices are supported:
  • Futronics FS-80 fingerprint USB-scanner
  • BioLink U-Match 3.5 fingerprint USB-scanner
  • BioLink U-Match 7.5 fingerprint USB-scanner
  • BioLink U-Match 5.0 fingerprint USB-scanner (with a card reader)
  • UPEC fingerprint scanners
  • BioLink i-Match 2.0 iris USB-scanner

6. **IDenium Maintenance**

IDenium is a user-friendly solution and does not require any special skills, long-time 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 Active Directory Users and Computers snap-in).

6.1 **Logging**

IDenium has a built-in logger, which provides administrator-friendly access to all events happened within the IDenium system.

These events comprise the following:
• User creation
• Biometric identifiers enrollment
• User authentication and access to the targeted operating system
• Synchronization of user accounts and other IDenium-related data
The IDenium log can be viewed using standard **Computer Management** console. The logger allows monitoring IDenium system health status, locating, tracing and eliminating errors, obtaining supplemental information about IDenium operations and performing other IDenium maintenance tasks.

### 6.2 Uninstallation

IDenium software can be completely uninstalled in case you want to revert to your previous configuration. It is supposed, that IDenium client components should be uninstalled first; only then, IDenium server software may 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 scheme from back up (losing all changes made after the date, when back up was created).

### 6.3 Support and Troubleshooting

Please feel free to contact Bio-Metrica Technical Support Department team at technical.support@bio-metrica.com

### 7. Where to Find Additional Information

Additional information about IDenium as well as other products and solutions can be found at [http://www.bio-metrica.com](http://www.bio-metrica.com)

Bio-Metrica is the authorized distributor of IDenium and other Biolink products for the Americas.