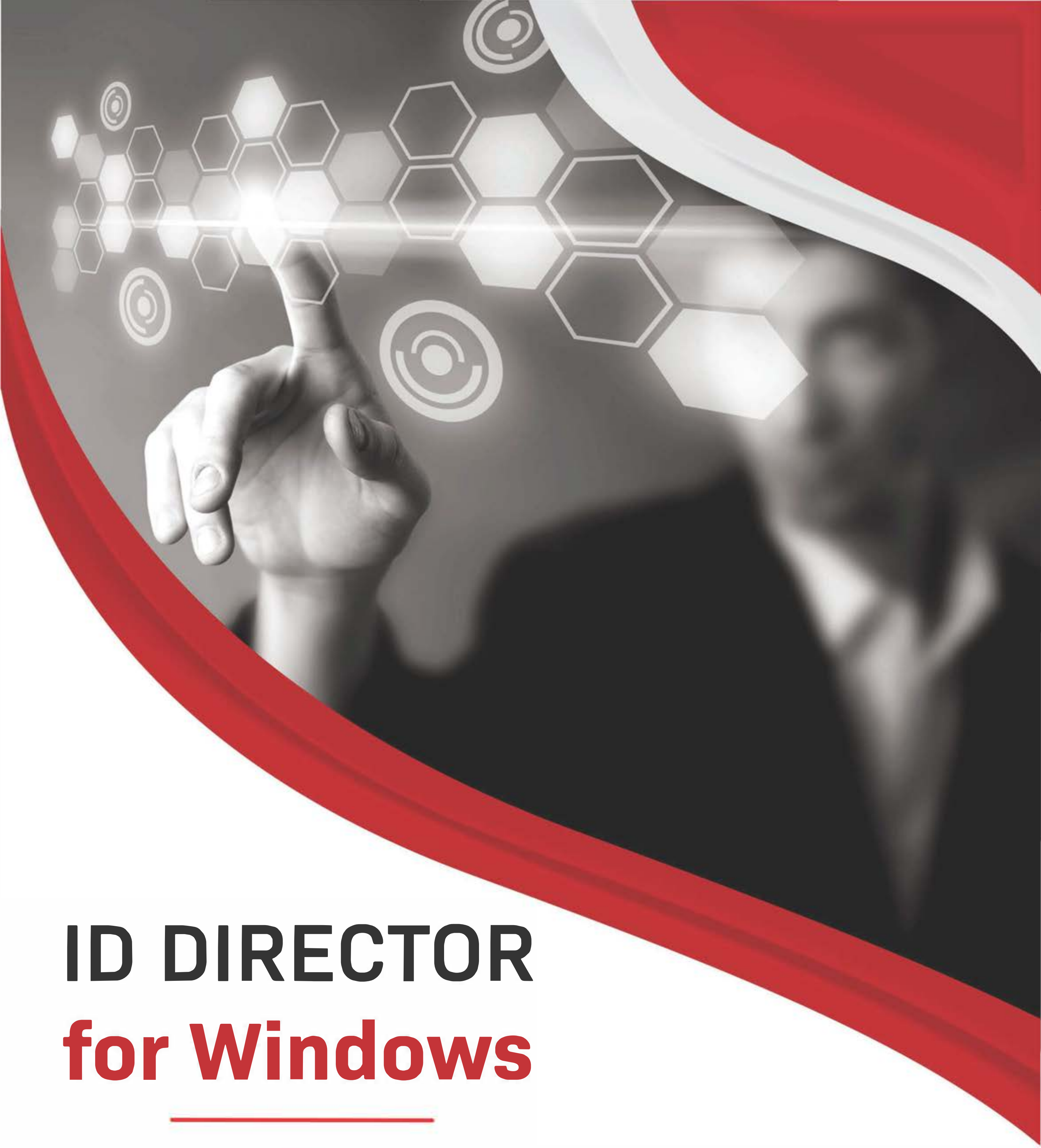


ID DIRECTOR
for Windows

BIO-key™
The Power of a Touch

☎ **Phone**
O:(732) 359-1100
F: (732) 359-1101

✉ **Contact**
info@bio-key.com
www.bio-key.com

Adress
3349 Highway 138
BLDG A STE E
Wall, NJ 07719

Microsoft
Partner

Introduction

Fingerprint biometrics are commonly deployed by organizations seeking to comply with authentication requirements and to reduce security risk and cost associated with user-selected passwords. Fingerprint biometrics are used around the world and are considered one of the more secure forms of identifying human characteristics and applying them to authentication. Fingerprint biometrics matches a known fingerprint template with that presented by a user at the time of an authentication request. ID Director for Windows® (IDfW) manages the lifecycle of fingerprint biometrics by capturing a user's fingerprints and creating reference templates during enrollment and also supports the enrollment of a user selected PIN (or AD password) to be used as a second factor of authentication.

Fingerprint templates are encrypted and stored on the IDfW Server. The common logon workflow for using fingerprint biometrics requires the user to present or swipe one of their enrolled fingerprints on a sensor; once recognized the user may be required enter the associated PIN or Active Directory® password, which is then compared to the information stored on the IDfW Server. Once a successful match is verified, the user is permitted access to the operating system and applications.

Overview

BIO-key ID Director for Windows® is an advanced authentication software solution designed to support biometric fingerprint login to Windows® for Microsoft® Active Directory® domain users. This technology allows users to enroll a fingerprint biometric credentials into a secure, centralized repository, and authenticate to a Microsoft® domain from any authorized Windows® device using their domain username and a fingerprint only, fingerprint + PIN, or fingerprint + domain password, depending upon the security policies enforced for the device. IDfW supports fingerprint authentication on dedicated workstations as well as shared workstations and kiosks. Computers may be connected to the corporate network via LAN, WAN, or VPN with access to the authentication servers and domain controllers, or they may authenticate offline using an encrypted local cache, to allow full support for mobile users.

Supported Platforms

Users can perform fingerprint authentication on all currently supported Windows® operating systems, including Windows® 7, Windows® 8.1 and Windows® 10 desktops, as well as Server 2008 R2, Server 2012 R2, and Server 2016. ID Director for Windows® is integrated into Windows® as a Credential Provider (CP), which supports the use of fingerprint for primary authentication, as well as other system authentication scenarios where the Windows® Credential Provider is presented for login to AD. Some examples of this are seen when connecting to Remote Desktop Services (Terminal Services) when running applications that require administrator-level permission required by User Account Control (UAC) settings, when running applications using "Run as Administrator," when accessing network resources, or any time the Windows® Security window is presented. Any Microsoft® or custom applications that support or require authentication to AD via the Windows® Credential Provider.

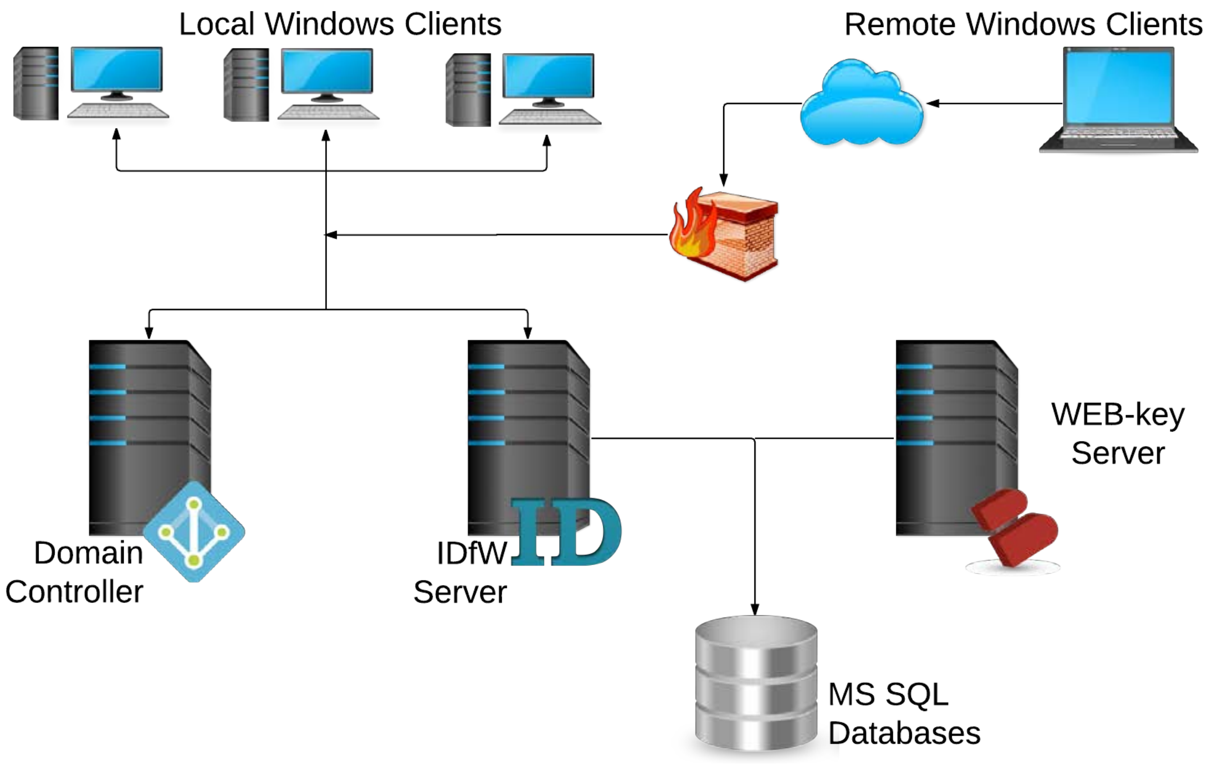
Architecture

ID Director for Windows® is implemented in a client-server architecture that allows for servers to be deployed where necessary to support scale and performance requirements. The server- side consists of the web-server components (web services site, Administrative Portal and User Portal) deployed on Microsoft® Internet Information Server and a Microsoft® SQL database.

The web components and the database may be deployed in a simple, single-server architecture, or distributed to leverage high availability and redundancy. In a large-scale deployment, multiple authentication servers are deployed behind load balancers and configured to leverage MS SQL deployed in various AlwaysOn fail-over modes. Authentication servers (or the web- services components only) may be deployed in a DMZ to support remote and mobile clients.

Multiple authentication servers may further be deployed (with or without a load balancing system) having individual web services URL's configured for a domain or OU where desired for geographical, functional, or other organizational structure defined within Active Directory®.

The Clients communicate to the authentication servers through REST-compliant web services. All communications between the IDfW Client and Server utilize standard HTTP / HTTPS protocols and standard ports so that no special firewall rules are required. The client will capture the fingerprint from the user, match the sample against the enrolled fingerprint templates stored on the server (or local cache if the client is offline); once the user's fingerprint has been verified, the client CP will package the credentials for interactive and domain login.



Active Directory® Integration

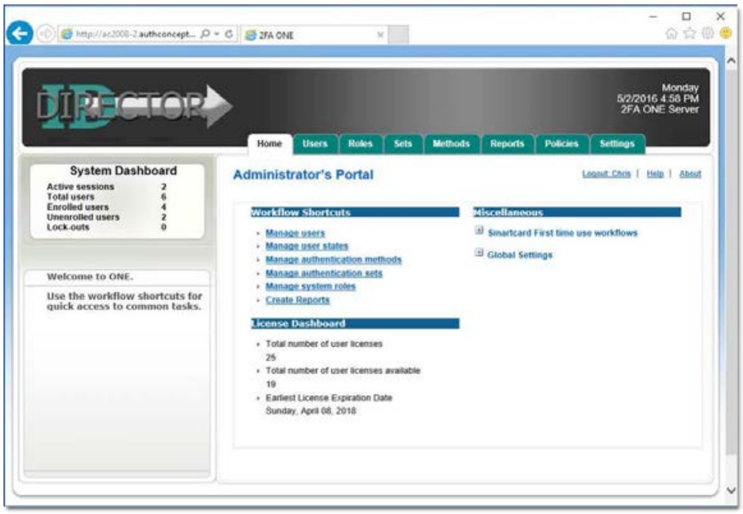
ID Director for Windows® is tightly integrated with Microsoft® Active Directory® to make administration tasks simple and to provide a familiar interface to the IT department. Managing users and computers is accomplished using the same domain and Organizational Unit (OU) hierarchy structure and inheritance as in the AD Forest.

BIO-key integration with Microsoft® Active Directory® is designed to be low-impact, efficient and secure. IDfW servers may publish Service Site URL information to AD requires but does not require schema modification or other permanent changes to AD. There are significant benefits to the overall health of Active Directory® by restricting the size and amount of data needed to replicate between domain controllers and across multiple sites. All fingerprint template data, configuration data, and policies are stored in the MS SQL database, to eliminate any performance impact on AD.

The domain controller (DC) role does not change following implementation of ID Director for Windows®, and DC's will continue to provide the ultimate authentication, authorization and access control of the user on the domain. Following a successful biometric verification, the domain password (hash) will be provided to the domain controller through the Password Credential Provider. Therefore, the domain password will continue to exist, and according to policy, be subject to expiration and change. Password change messages will still be presented to the end user, and the end user must perform password change. It is not expected that the user remembers their current (old) password; therefore, IDfW will provide the old password so long as the biometric verification is successful. The user may either select their new password, or BIO-key can generate a randomized password. An administrator may still change passwords in AD Users and Computers console, or other Microsoft® or 3rd party password management tool.

Administration

All user and computer administration is performed via the IDfW Administrator Portal delivered through a web interface accessible on the server(s) or via any administrative workstation with Internet Explorer. Administrative rights are defined as Roles, that determine which configuration settings an administrator may access in the system, how credentials may be managed for users, and which users may be administered (including other admin Roles). This allows for tight controls over administrator access levels while allowing lower-level administrators to perform everyday tasks such as enrolling users, or slightly higher-level tasks such as unblocking user accounts. Administrator Roles can be mapped directly to existing Security Groups in Active Directory®.



Monday
5/2/2016 4:58 PM
2FA ONE Server

System Dashboard

Active sessions	2
Total users	6
Enrolled users	4
Unenrolled users	2
Lock-outs	0

Welcome to ONE.

Use the workflow shortcuts for quick access to common tasks.

Administrator's Portal

Workflow Shortcuts

- Manage users
- Manage user states
- Manage authentication methods
- Manage authentication sets
- Manage system roles
- Create Reports

License Dashboard

- Total number of user licenses
  25
- Total number of user licenses available
  19
- Earliest License Expiration Date
  Sunday, April 08, 2018

Miscellaneous

⊞ Smartcard First time use workflows

⊞ Global Settings

(Image: Administrators Portal)

Computer Policies

Computer policy management provides over 70 configuration settings that allow for full control over the behavior of the IDfW Client deployed to domain computers (Policies cannot be attached to non-AD joined computers, the settings would have to be configured locally). As with other administrative tasks, policies are configured for AD domains, OU's and computer objects. Computer policy administration is simplified through the embedded AD Lookup Tool that provides a graphical administrative interface similar to Microsoft® AD Users and Computers, delivered through Internet Explorer as an ActiveX® control.

Client policies control the Windows® login experience, including which Credential Provider tiles are displayed or hidden (i.e., Fingerprint Login, Password Login, Enrollment). Other client policies control the user experience, and grant/suppress access to various components of the client and to control other security features of the client, such as the ability to authenticate offline to the local cache.

Synchronization of policies between clients and servers may be configured to support connectivity speeds and response times, as well as specific policies for remote users that required connectivity through a VPN. Hardware options may be configured to define support for fingerprint biometric and non-biometric authentication methods, as well as the mode of operation for fingerprint authentication. IDfW can be configured to support a 1:1 biometric verification method, where the username is required during authentication, or "1 to many" biometric identification that will allow one-touch authentication, with only a fingerprint.

User Policies

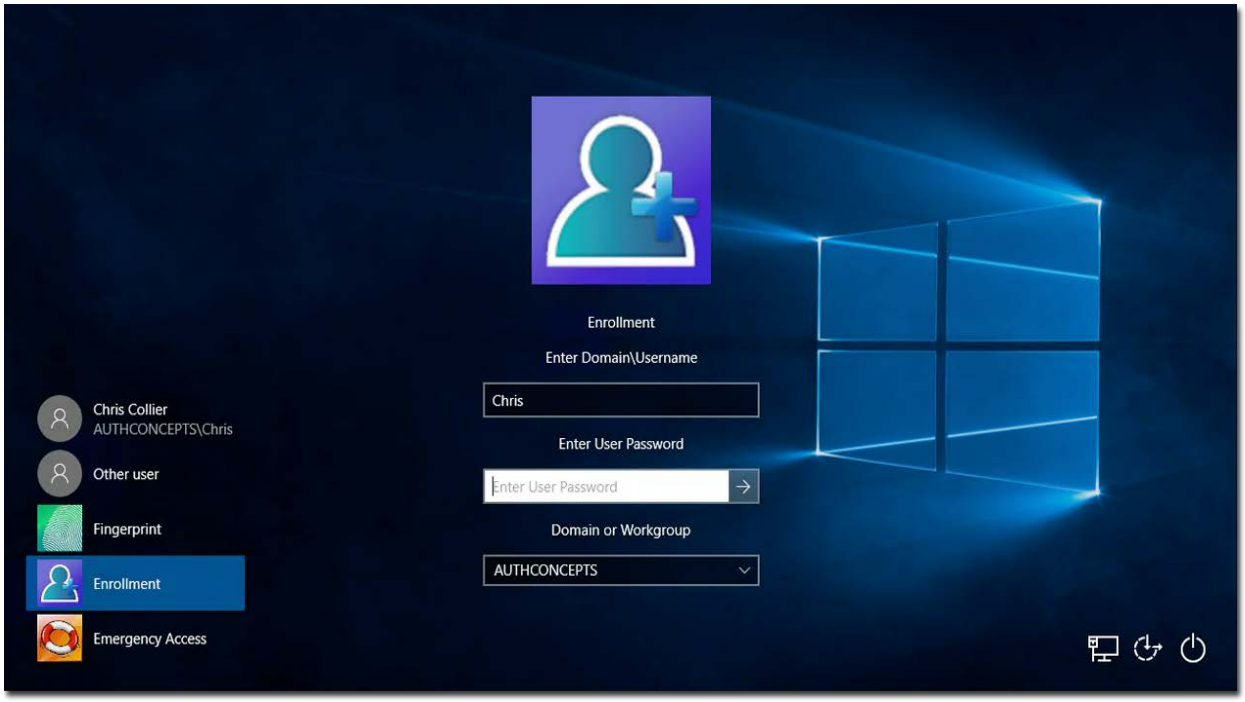
User policies are configured to define the behavior of the advanced authentication methods implemented within the system. Standard policies for fingerprint authentication includes the number of fingers that are required for enrollment, as well as PIN policies. PIN policies involve the support of unique PIN enrollment that may be enrolled for use at Windows® login or Windows® unlock, as a second authentication factor, in addition to the fingerprint. Another common policy is to require the AD password, in addition to the fingerprint at login or unlock.

User management is simplified by providing an AD Lookup Tool to browse AD Domains, OU's and Security Groups to perform bulk administration tasks or to search for specific AD users. Full user state and credential lifecycle management is performed to add/import users, reset or replace credentials, unblock credentials, disable and delete users within the system.

Administrators may run reports on users to visualize, qualify and quantify who has successfully enrolled, who are not enrolled, or who may be blocked due to failed login attempts. The IDfW Administrator Portal also allows for managing unique policies for different users based on Security Group or OU; as with computer policies, specific users may have different policies enforced to define which credentials must be used, and how they must be used.

Fingerprint Enrollment

Enrolling fingerprints into the IDfW system is a critical step in the life-cycle of the credential, and enrollment should be of the highest possible quality to ensure the success of all subsequent authentication requests. Fingerprint enrollment must be made available to all users, regardless of location, including remote and SOHO users. Therefore, IDfW provides multiple enrollment methods to support centralized enrollment via Internet Explorer browser at designated Enrollment Stations as well as self-enrollment via an Enrollment Credential Provider available on any authorized Windows® workstations. All enrollment methodologies are secure workflows, which require the enrolling user to authenticate using their domain credentials.



Enrollment

Enter Domain\Username: Chris

Enter User Password: Enter User Password

Domain or Workgroup: AUTHCONCEPTS

During the enrollment process, the user is prompted to enroll one or more fingers, as defined by policy (common policy requires 2-3 fingers). Four samples of each finger are captured to create the VST template, ensuring that the maximum amount of data is collected from each finger before processing. Once the required number of fingers is enrolled, the user may be required to create a PIN (optionally as defined by policy). All enrolled credentials are immediately encrypted and stored by the IDfW server in the SQL database. Once enrolled, users may authenticate using the centrally stored biometric credential at any workstation where the IDfW Client is installed.

Secured Applications

Secured Applications provides single sign-on functionality that extends the benefits of fingerprint authentication to applications and IE websites that rely on username and password login. The IDfW Client can be configured by an administrator to identify login, change a password, and other secure workflows, where the Client may intercept the login request and prompt the user for their fingerprint (as well as a PIN or AD Password if desired). Upon successful authentication, the application's unique or AD credentials are supplied, and the user is logged in. This extends the security benefits of using a fingerprint to every application, while not requiring any change to the application; therefore, integration is fast and straightforward and incurs no additional cost.

Shared Workstation

Shared Workstation is an operational mode of ID Director for Windows® that allows the fingerprint authentication to be enforced on shared and kiosk systems where the Windows® OS uses a generic login. The result is a fast-user-switching computer where users are required to authenticate with their fingerprint, against Active Directory®, before they have access to the desktop. IDfW in Shared Workstation mode may be configured to auto-launch and login to common virtualization technologies such as Microsoft® Remote Desktop Services, VMWare vSphere® and Citrix XenDesktop®. Shared Workstation works with Secure Applications to provide fast and secure access to applications without requiring users to login/logout of Windows®. This is a common use-case in healthcare, law enforcement, retail and numerous other, often regulated, environments where the implementation of strong authentication must not impact the speed of access.

Reader Hardware

BIO-key supports approximately 50 fingerprint reader devices from over 20 manufacturers. Many BIO-key fingerprint hardware partners have adopted, or are migrating towards the driver standards provided by Microsoft® as part of the Windows® Biometric Framework (WBF).

Hardware drivers for WBF compliant readers are automatically downloaded and installed by Windows® Update, and BIO-key provides many proprietary driver packages to simplify the hardware deployment process and facilitate driver updates. There are three primary types of fingerprint sensors, supported by BIO-key, that utilize unique methods of capturing fingerprint images from the user.

- Optical fingerprint sensors capture a digital image of the fingerprint using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) which captures a visual image of the fingerprint.

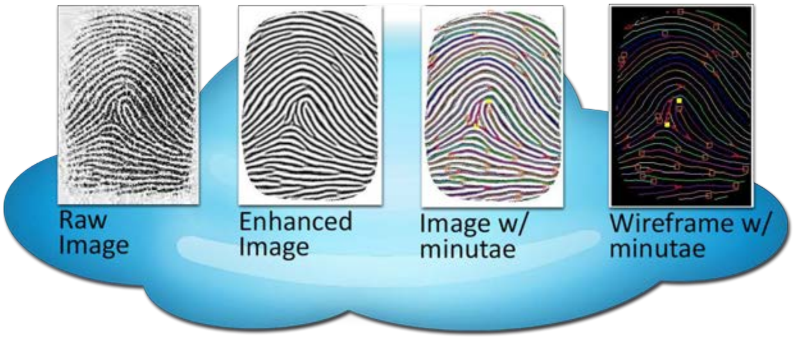
- Capacitance sensors use principles associated with capacitance to form fingerprint images. In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric. A passive capacitance sensor uses the principle outlined above to form an image of the fingerprint patterns on the dermal layer of the skin.

- Ultrasonic sensors make use of the principles of medical ultrasonography to create visual images of the fingerprint. Ultrasonic sensors use very high-frequency sound waves to penetrate the epidermal layer of skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials. Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint.

Regardless of hardware manufacturer and drivers, BIO-key utilizes a common biometric template, created using Vector Segment Technology (VST), to ensure full interoperability between reader devices.

Fingerprint Algorithm

ID Director for Windows® includes BIO-key's patented Vector Segment Technology (VST), vector-based fingerprint algorithm. VST achieved the highest overall ranking in key accuracy metrics among commercially- available products for false acceptance (FAR) and false rejection (FRR). VST exceeded the U.S federal government's FAR standard by a factor of 10, resulting in fewer than one in 10,000 erroneous matches. This is achieved through processing raw fingerprint images through over 40 levels of enhancement and extraction of over 1,200 unique data points to create a highly discriminate template captured and stored at enrollment and later compared for a successful match during authentication. The data points are comprised of unique identifying characteristics and patterns of a fingerprint, which can be computed into the mathematical model (template) for highly accurate comparison.



A highly unique, and precious result of implementing the BIO-key algorithm into the Windows® authentication workflow, is the ability to perform "true" large-scale 1 to many identifications of users. This provides the ability to authenticate to a dedicated, shared, or kiosk workstation using only the fingerprint to identify the user and authenticate the user against Active Directory®. This feature is critical in certain environments, such as healthcare, large call centers, retail and others where ease of access to large numbers of shared workstations is equally vital to security requirements.

A highly unique, and precious result of implementing the BIO-key algorithm into the Windows® authentication workflow, is the ability to perform "true" large-scale 1 to many identifications of users. This provides the ability to authenticate to a dedicated, shared, or kiosk workstation using only the fingerprint to identify the user and authenticate the user against Active Directory®. This feature is critical in certain environments, such as healthcare, large call centers, retail and others where ease of access to large numbers of shared workstations is equally vital to security requirements.

This workflow is supported through the accuracy provided by the VST algorithm combined with the indexing capabilities and highly configurable search profiles. The process begins at the client, where the fingerprint image is captured, processed, and converted into a template (model) for comparison. The template is sent to the server to be identified. The server implements a layered index approach to identify which templates are the most active candidates for a match based on multiple characteristics of the print. Each layer represents a smaller sample of the total database, and at each layer, the quality of the potential matches is increased as the number of candidates reaches a specific threshold, i.e., 10 – 100 possible matches, a full template comparison can be made until a single, unique match is identified. The user identity associated with that match is then returned, along with the user's AD credentials, to complete the authentication process.

BIO-key's Vector Segment Technology allows this process to occur extremely quickly, allowing the identification time to appear nearly instantaneously to the end user.

Additional Authentication Methods & RADIUS

In addition to fingerprint biometric authentication, ID Director for Windows® provides support for other primary authentication methods that can be implemented for Windows® authentication, as well as authentication into other BIO-key products and other commercial solutions that support the RADIUS authentication protocol through Microsoft® Network Policy Server. The most common methods of authentication in these categories are One-Time- Password (OTP) and newer "Out of Band" technologies that push an authentication request to a mobile device, such as a mobile phone.

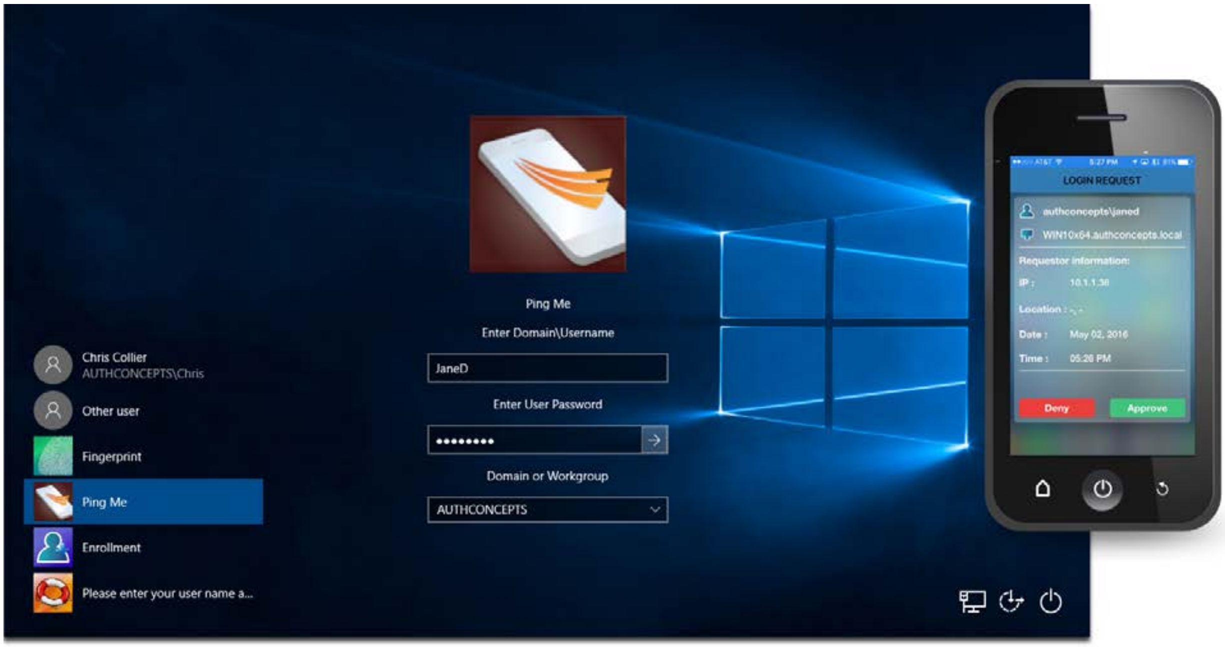
One-Time-Password

For OTP authentication, the user carries a small "key fob" device with an LCD display or an app installed on their mobile device. Supported platforms for the BIO-key OTP app are Windows® Phone, Android and iOS. During authentication to Windows®, VPN, or other application, the user is prompted for an OTP (or AD password + OTP), and the user has a specific amount of time to supply a six-character passcode to the requesting application. The OTP passcode is typically generated by pressing a button on the key fob, or by authenticating to the mobile app through the use of a PIN or fingerprint. The IDfW server validates the OTP value either from a native process between BIO-key Client and Server or from 3rd party application RADIUS request to MS NPS Server.

PingMe

Newer trends in technology have allowed a similar authentication process to occur for Windows®, RADIUS, etc. as described above using OTP, through the use of out-of-band authenticators that send (or “push”) the authentication request directly to an end user’s mobile device to allow the user to “Accept” or “Deny”. This eliminates the need for the user to initiate the authentication process in two different places:

1. Application authentication request, and
2. OTP devices or app. PingMe offers a higher level of security than early-generation SMS passcodes, and simplifies the process, as the user may respond to the authentication request on the mobile device; once authenticated, the user does not need to type in an OTP passcode or provide any additional input into the application, which receives the validation “out-of-band”, and allows the user access.



Ping Me

Enter Domain\Username: JaneD

Enter User Password: ••••••••

Domain or Workgroup: AUTHCONCEPTS

LOGIN REQUEST

authconcepts\janed

WIN10x64.authconcepts.local

Requestor information:

IP : 10.1.1.38

Location : -, -

Date : May 02, 2016

Time : 05:26 PM

IDfW on Microsoft® Azure

ID Director for Windows® may be deployed on virtualized hardware, including Microsoft® AzureTM. The authentication server and database components have been validated on the Azure platform to deliver the same functionality and security as an on-premise deployment. ID Director for Windows® may be deployed on a Microsoft® AzureTM Domain as well to allow biometric authentication against AzureTM AD in the same fashion as a corporate domain, leveraging all of the benefits of this platform.

Data Security and Encryption

All credential data is secured by IDfW while at rest, and while in transit using FIPS 140-2 compliant encryption algorithms and hash functions. Data stored in the SQL database and local cache are encrypted using AES 256, while network data leverages 3DES. Additional network encryption may be implemented using SSL between the IDfW Clients and Servers. Unique keys are managed by the systems to ensure that each user and computer in the deployment are individually protected, and so that if a key were compromised from one machine that it could not be used to access data on another computer.

While all data must be decrypted to be accessed, this is all performed in protected memory where Sensitive data is encrypted at all times, except for the exact time it is needed for the ‘just-in-time’ algorithms. Immediate removal is done using a secure wipe of those addresses in memory. This ensures that the data is not left residing in decrypted form after it is no longer needed. The technique protects explicitly against in-memory attacks as well as those against the RAM chip.