
Bioscrypt VeriSoft Access Manager: An Integrated Approach to Solving the Security Dilemma



- Executive Overview2**
- Introduction3**
 - The Case For Unified Security 3
 - Challenges..... 4
- VeriSoft Access Manager Components5**
 - VeriSoft Access Manager Server 5
 - VeriSoft Access Manager Client..... 7
- The VeriSoft Access Manager Client Technology Portfolio.....9**
 - Introduction..... 9
 - Network/Desktop Login 9
 - Single Sign-On 10
 - Application Protection 13
 - Encryption..... 13
- Architecture..... 14**
 - Introduction..... 14
 - Multi Factor Authentication..... 14
 - Directory Support 19
 - Communication and Encryption 20
 - Dynamic Role-Based Policies 20
 - Delegated Administration 22
 - Auditing..... 23
 - Standards..... 23
- For More Information24**

Executive Overview

As computers are getting increasingly mobile and better connected, threats to data security are increasing in number as well as complexity. Business customers, for whom data security can have a direct impact on the health of their business, are becoming increasingly concerned about this problem. Bioscrypt understands that security needs must be addressed holistically. It has developed a solution which brings together many identity verification technologies in a way that not only ensures protection of client data and devices, but also ensures that users themselves do not become points of vulnerability to the entire IT infrastructure.

This proactive solution from Bioscrypt is called VeriSoft Access Manager. Not only does it meet the requirements of today's IT security needs, but it is also extensible and therefore able to grow to handle new threats. As new requirements emerge, the tools and components to meet them will easily integrate into the product.

Introduction

VeriSoft Access Manager provides a robust client/server capability which consolidates multiple user application credentials into a single, secure Identity. This protects against unauthorized access to sensitive user data or applications.

Although not required, the inclusion of fingerprint verification technologies can significantly enhance the security of the VeriSoft Access Manager solution. With the right solution, enhanced client security and a unified user identity can provide the following benefits:

- Increased security for the client PC through fingerprint, multi-factor, and hardware-based authentication
- Credentials remain protected by virtue of hardware based encryption, protecting even if the hard drive is removed
- Users need only remember a Single access policy when accessing sensitive data protected by strong encryption (e.g. TPM encrypted user data)

Longer term, hardware platforms with embedded security modules will be a requirement of the next generation of security architectures. As customers consider long term strategies for incorporating this technology into their environments, choosing an enterprise credential and SSO (single sign-on) management solution that provides hardware based protection capability becomes an important consideration. VeriSoft Access Manager fully integrates existing security architectures with user directories and complex password policies.

The Case For Unified Security

Developers of Enterprise Systems have struggled with providing a unified interface for their security infrastructure, including authentication, Single Sign-On, policy management, administration, and auditing. The Gartner Group, a leading industry analyst firm, makes the following statement in regards to enterprise security services and authentication:

“The Gartner Group reports that the market for network security services totals more than \$6 billion and is doubling every year. In particular, managing the multiplicity of passwords required for user identification is one of the most labor-intensive and risk-prone areas of IT operations. Both Forrester and Gartner have concluded that the cost of managing passwords within the enterprise ranges from \$150 to \$300 per user per year. In fact, password problems are the #1 cause on help line calls.”

Organizations looking to drive this cost down are looking to address several security issues, including:

- Increased number of disparate applications being used in the enterprise – each with a proprietary authentication mechanism and directory.
- Inherent need to provide a better level of non-repudiation for user access within the enterprise – including federal mandates such as HIPAA and Sarbanes Oxley.
- Dissatisfied end users who deliberately attempt to bypass system security requirements.

Challenges

While there are many advantages of implementing secure authentication and credential management into a practical enterprise environment, it does not come without challenges. Some of the challenges include:

Complexity – Heterogeneous enterprise systems involve a collection of complex and independent computer systems, each with its own security requirements, interfaces, and related management requirements. The integration of several independent systems presents a considerable technological challenge.

Availability and Portability – In order to provide a secure authentication and credential management infrastructure, the credential information needs to be accessible as well as secure for each user. The enterprise administrator needs to ensure that secure access to all services is available regardless of network connectivity or server load.

Flexibility – Enterprise security requirements will differ from one department or organization to the next. Some enterprise administrators will require several authentication methods and strict policies. These are often based on federally mandated requirements or upper management directives. Other enterprise administrators may just be looking for a solution which provides better 'ease of use' of their existing enterprise systems. A robust solution is one that is flexible enough to handle the easiest configuration as well as the most robust architecture requirements. It is imperative that it work across multiple organizations as a unified product.

The VeriSoft Access Manager's Technology Portfolio addresses all of these challenges by providing a tightly integrated framework and a modular, unified approach to configuring and integrating security policies, authentication methods, and enterprise applications. The client/server architecture discussed in the following section lays the foundation for these technologies.

VeriSoft Access Manager Components

VeriSoft Access Manager Server

VeriSoft Access Manager is a tightly developed framework that brings several different security technologies together into a unified User Identity. The VeriSoft Access Manager Server gives administrators the ability to specify how different security policies will work together to provide access control to authorized clients. These policies can include advanced authentication methods (Smart Cards, Biometrics, USB Tokens, Trusted Platform Modules (TPM) and other future technologies), time and date, user directories, platform security, TCP/IP addresses, ports and protocols, and more. With VeriSoft Access Manager Server, administrators can create a unique security policy that requires their chosen authentication method, including alternatives to passwords when logging on to Microsoft Windows.

Password management is a complex task that involves the memorization, protection, reply, error correction, synchronization, reset, and randomization of user credentials for multiple enterprise applications. VeriSoft Access Manager also provides a Single sign-on capability that automatically remembers and manages user credentials for websites, applications, and protected network resources. VeriSoft Access manager is effectively a user identity vault that makes accessing protected applications more secure and convenient.

The VeriSoft Access Manager Server uses the corporate directory for the storage of encrypted user credentials and for maintaining the server database (which includes the server administration, authentication policies, and configuration options). The VeriSoft Access Manager has no need for a proprietary database; multiple LDAP repository architectures are supported allowing for deployment anywhere, while leveraging existing investments in corporate directory architecture.

Key features of VeriSoft Access Manager include:

- Fully integrated universal security client supporting multiple applications.
- Multi-factor authentication server with support for Smart Cards, Biometric fingerprint security, USB Tokens, Virtual Tokens and Passwords.
- Single sign-on capability protects passwords for websites, applications and network resources.
- Support for Trusted Platform Module (TPM) embedded security chips which provide strong, hardware-based encryption protection for the user's identity store.
- Secure access to Terminal and Citrix MetaFrame servers using the entire set of authentication methods and policies provided in a 'FAT' environment.
- Remote Access support for Dial-Up and VPN connections.

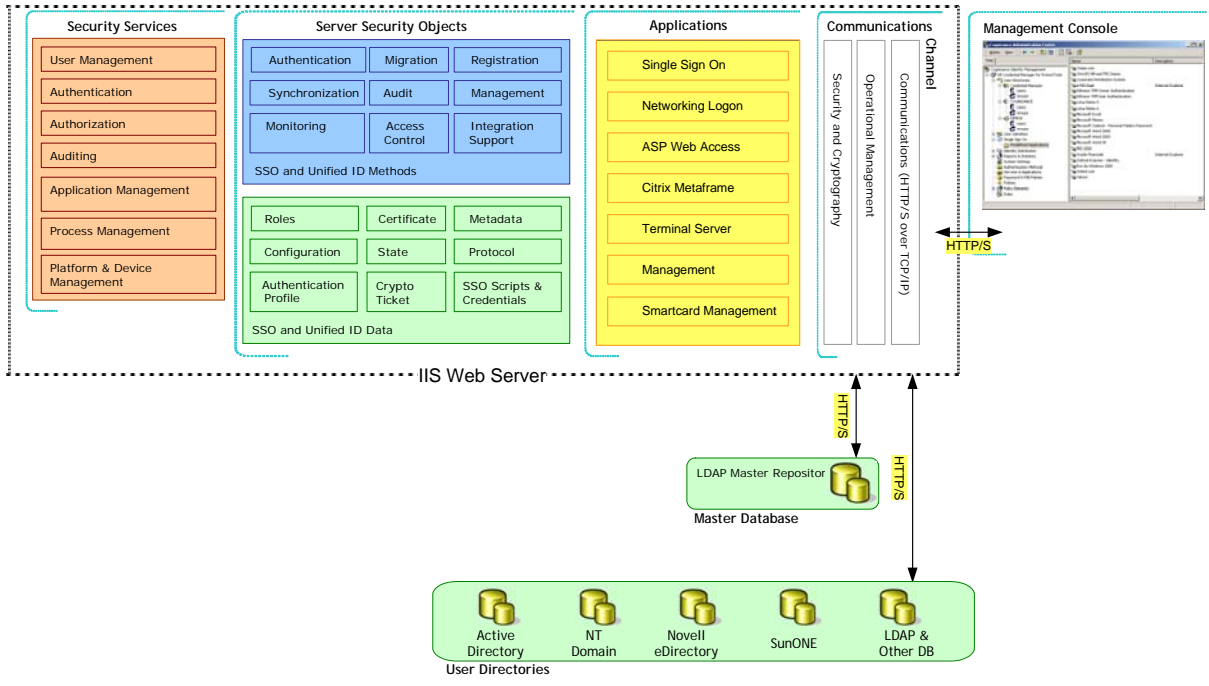


Figure 1 - VeriSoft Access Manager Components

VeriSoft Access Manager Client

The VeriSoft Access Manager Client is the front end that accesses all of the secure credentials and components stored within the user's Access Manager 'Identity'. The Client provides enterprise network logon as well as a "launchpad" of services and applications enabled specifically for the user based on a set of robust and dynamic policies put forth by the administrator. The stored Identity of the user tells the client how, when, and where a user can log on, and provides his credentials for Single Sign-On throughout his enterprise after logon.



Figure 2 - VeriSoft Access Manager Client

Only authenticated users can access and unlock encrypted credentials within the user's Identity. Strong authentication can be achieved via a wealth of choices including various hardware authentication devices, software-based strong authentication, and role based access to the VeriSoft integrated applications. This provides flexible deployment options and increased security and productivity, while maintaining user acceptance and usability.

The VeriSoft Access Manager Client functionality is available both to individuals (for personal credentials storage) and for corporate usage (for corporate credentials and applications protection.) Policies for application access, single sign-on, and network logon are easily configurable by the administrator. Pre-defined policies and automatic or random password management come built in. Users may also self-service their personal settings.

The following figure outlines the various components of the VeriSoft Access Manager Client.

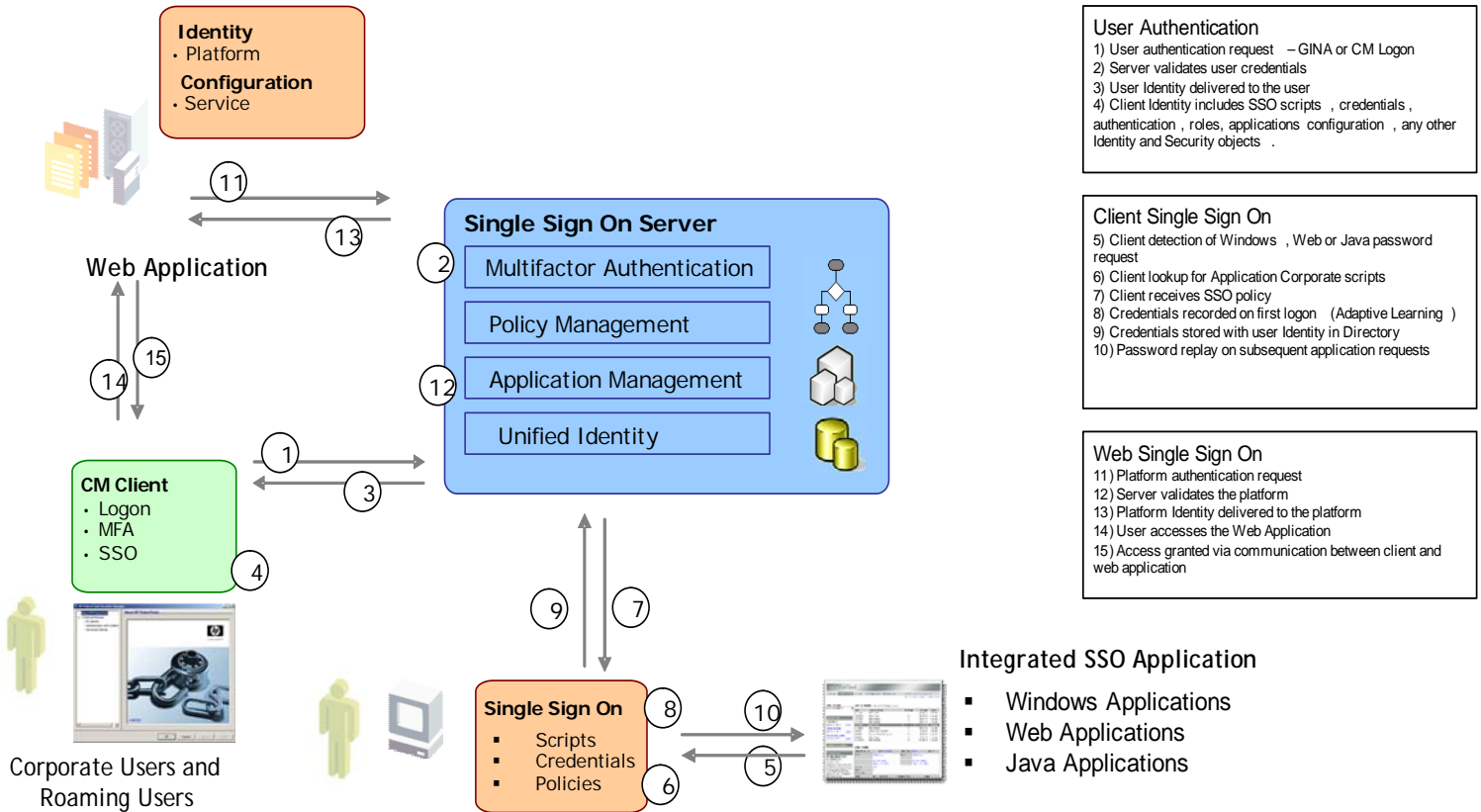
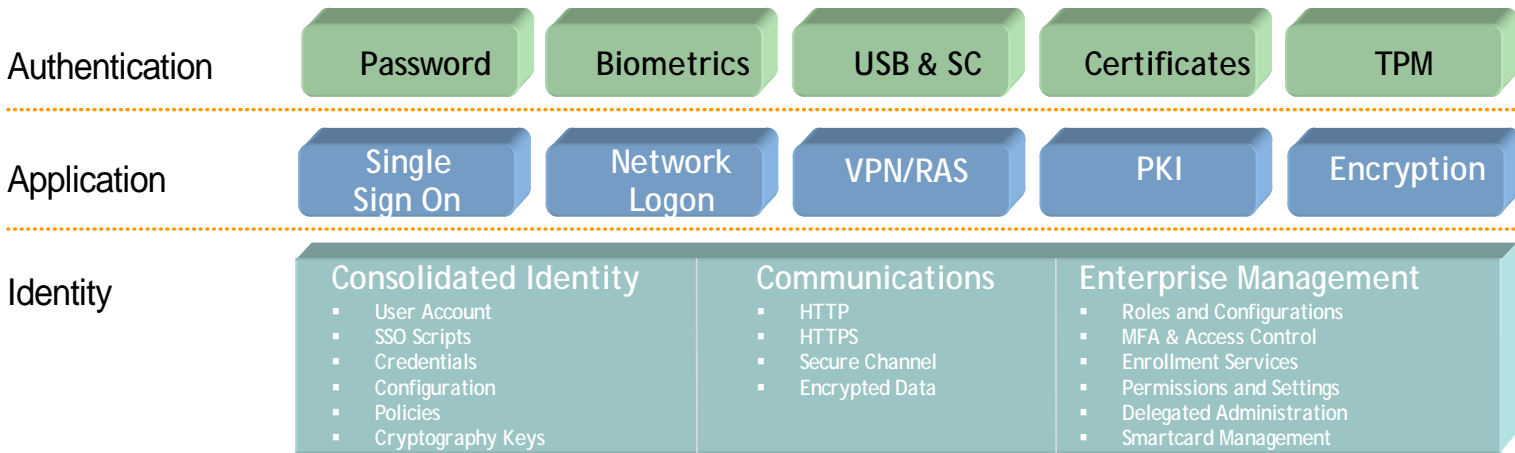


Figure 3 - VeriSoft Access Manager Client Components

The VeriSoft Access Manager Client Technology Portfolio

Introduction

The VeriSoft Access Manager Client contains a tightly integrated, modular suite of software solutions for enterprise security deployment. VeriSoft features a range of applications that provide enterprise scalability with simple management interfaces. What separates VeriSoft Access Manager from other solutions is its tight integration and seamless user interface, rather than several disparate applications designed to solve the same enterprise problems.

The following sections outline each of the major technologies contained in the VeriSoft Access Manager Suite.

Network/Desktop Login

The VeriSoft Client provides a customized login interface as a replacement GINA (Graphical INterface for Authentication). This provides additional security to your desktop or enterprise logon at the system level. With VeriSoft, users may logon using advanced authentication methods and associated policies—more than what is supported inherently by the operating system. An enterprise administrator can now chose from the following sign-on methods: Fingerprint, Smartcard, Token, Certificate, Trusted Platform Module, or several other authentication methods.

The VeriSoft Access Manager Client works with the VeriSoft Access Manager Server and the existing enterprise directory to centrally manage the user accounts and associated credentials and policies. When the proper credential(s) are provided to satisfy the logon policy, VeriSoft Client provides secured access to both Windows and Novell Networks.

Additional authentication methods allow the VeriSoft Access Manager to manage passwords for network logon and Single Sign-On. VeriSoft has the ability to change passwords behind the scenes automatically. This adds an additional layer of security whereby the end user does not know their password for an enterprise logon and will not be able to access the enterprise without a proper alternate credential. This means that when the user tries to logon to a workstation with or without the VeriSoft client, they will be unable to log on without additional credentials, thus ensuring that the users do not become a weak link in the security chain.

Single Sign-On

User authentication for legacy systems is a major administration problem for most organizations. The abundance of applications with proprietary authentication systems requires individual users to memorize a growing number of credentials.

A password's effectiveness as an authentication method erodes under most companies' security policies. An organization can no longer reasonably expect its users to remember long lists of username and password combinations. The average user in today's large enterprise utilizes five to fifteen major systems, many of which have their own authentication systems. Most users will rely on easy to remember passwords that are duplicated throughout these systems, or write passwords down in a location close to their computer to avoid memorization.

Enterprise Application Password Management

To reduce the burden of password memorization that lies on end users and the associated required management by organizations, VeriSoft Access Manager's Single Sign-On feature provides a secure way to store user credentials for all applications within the enterprise realm. Storage of the user credentials and the automatic submission of passwords for the user when it is required eliminate the need for username/password memorization as well as the tendency users have of writing them down.

VeriSoft Access Manager provides several solutions:

- The security problem of users compromising passwords due to limitations of memorizing long passwords is resolved.
- The number of calls to help desks concerning forgotten passwords is greatly reduced. This directly reduces costs of up to approximately \$300 per user per year (Gartner).
- Strong multi-factor authentication secures application credentials and provides automated application credential management.
- Productivity increases because users are not losing access to applications due to password problems.

Single Sign-on Application

The Single Sign-On application is a plug-in to the VeriSoft Access Manager client that provides secure, server-based application credential(s) storage and protection. With the VeriSoft Access Manager, users' multiple credentials for their enterprise applications are securely distributed throughout the enterprise and become available upon successful authentication to the VeriSoft Server.

The Enterprise Single Sign-On options include wizards for creating custom scripts, automatic login screen detection, password randomization, password synchronization, and self-service for an optional end user management of Single Sign-On settings.

Administrators can optionally give end users access to manage additional applications themselves. For example, if an end user has an online banking site or web-based mail that he doesn't want to have to type the password for, if the administrator allows it, he can tie his own separate applications like these to his same user Identity already being used for logon.

Enterprise Application Registration

The Single Sign-On application has several different methods for configuring a new application for use within the VeriSoft Access Manager. Each method designs a customizable XML script that can be used for future Single Sign-On access within VeriSoft:

Automated identification of a login window:

VeriSoft's Single Sign-On will look at the active window of the application in use and if it determines that there is a username/password within that window, it will attempt to automatically capture your credentials. If successful, a script for that application is now setup for use.

Drag-and-drop interface:

VeriSoft has an easy interface to identify the components of a login window. The user/administrator will drag an icon onto the controls of the window one at a time, such as the username and password fields, the OK, the clear button, etc. After identifying the window, the user attempts to submit credentials and the application will register the script.

Pre-Defined Applications

To ease Single Sign-On usage in an enterprise, it makes sense to take the time to Pre-Define all of the applications that the end users will need access to. Within VeriSoft's Single Sign-On, the setup of application scripts that were so easily done above can now be exported to the server as a 'Pre-Defined Script'. It will then be available for use by all users in the enterprise that require such a script. The administrator simply picks the users who use this pre-defined application and adds it to their Identity. The administrator also has the ability to enter credentials for the user at the server so that the user will never know their credentials for the particular application.

Many-to-Many

Many-to-Many support refers to the ability of supporting multiple applications with multiple credentials sets, therefore allowing more sophisticated application handling. This includes several versions of one application, or several credentials for one application. An example of this case would be an enterprise CRM Administrator who has multiple accounts for the same application, including his separate 'Admin' account as well as his personal account. With Many-to-Many support, the administrator can store both accounts and passwords and prompt to specify which account to log on to during the application launch. The administrator still has only one identity, but multiple application credentials.

Interactive Authentication

Single Sign-On can provide an ease of use as well as security, but some enterprise administrators may be concerned that Single Sign-On actually enables security breaches by automatically submitting the application credentials. The VeriSoft Single Sign-On Application has the support to force a user to interactively authenticate to VeriSoft Access Manager before automatically submitting application credentials to an enterprise application, and this can be setup by a per-application basis for each user. Combining interactive authentication with a more secure authentication method requirement provides a level of security that an enterprise administrator desires.

Additional Action Support

While Single Sign-On can help to avoid entering a password, there are some “gotchas” that need to be considered. One example is a change password dialog. VeriSoft’s Single Sign-On application has the ability to learn how to handle these interfaces and can manage passwords behind the scenes. This adds additional layers of security to your enterprise systems.

Application Protection

An organization may desire to protect access to an application that may or may not require a username and/or password to grant access. Microsoft Group Policies only allow administrators to either allow an application to run or to not allow an application to run. VeriSoft Access Manager's Application Protection Plug-In fills in that gap by not only providing the ability for administrators to prevent end users from running specific applications, but also provides the ability to restrict the access to that application with an interactive authentication.

An administrator determines which applications are allowed, disallowed, or restricted based on user role throughout the enterprise. When the policy is defined, it is automatically applied when a user logs onto the system as a member of that role.

Example: A legacy CT Scan Viewer application in a hospital does not have a logon requirement. HIPAA regulations require an organization to be more secure when accessing patient data. Aside from regular windows policies, the Enterprise Administrator would like to ensure that only individuals that are supposed to have access to that application are able to use it. The administrator simply sets a policy of 'Restricted Access' to the CT Scan application for the roles allowed to access the application and leaves the policy active for 'Authenticate user each time application is used.' Every time the application is started, the user must successfully authenticate AND must be a member of the ROLE that is allowed access to the application.

Encryption

VeriSoft Access Manager provides the ability to create multiple secure drives and share encrypted information with multiple individuals. These drives may exist anywhere on a PC or network, including removable media – such as a USB drive. This encryption plug-in is known as the VeriSoft Document Manager within VeriSoft.

What is unique about this shared encryption is that because the Document Manager is part of a tightly integrated suite of products, VeriSoft can allow administrators and users to create secure disks and grant access to other members of the enterprise. These disks can be mounted in any of a number of locations and may only be mounted with proper authentication, based on the associated policy.

Architecture

Introduction

VeriSoft Access Manager is comprised of several different components that all tie together into a tightly knit framework. The flexibility and the robustness of the architecture are keys to the capabilities of the product. VeriSoft technology is based on industry standards and uses standard web-based protocols which allow management and usage over the internet.

The core idea behind the functionality of the VeriSoft Access Manager is the user's 'Identity'. Regardless of the amount of enterprise application logons a user may have, or how many directories he may be a member of – the fact remains that he is only one person with only one identity. VeriSoft follows that model by storing only one Identity and using that Identity to grant access to components within the system. That Identity will have all of the secured user information such as his/her authentication credentials, Single Sign-On Credentials, User Profile, and other pertinent Identity data.

VeriSoft works by using that identity throughout the enterprise and bringing it down to the user as he/she moves about the enterprise. The policies put in place via the VeriSoft Access Manager determine what can be done with that identity within the enterprise, but it is the VeriSoft Access Manager server which actively manages this information for the user. As users log on to a workstation, their identity is brought down to them. If the user logs off after making any identity changes, their updated identity will be returned to the server for the next use.

The VeriSoft Access Manager has very minimal requirements for operation and installation. The Server is installed on any machine running Microsoft Internet Information Server (IIS). VeriSoft uses IIS as the mechanism to handle communication of the HTTP and HTTPS requests back and forth from clients. Details of the communication and encryption used are discussed later on in this section.

There are a few key areas to focus on within the architecture, including the Multi Factor Authentication, Directory Support, Communication and Encryption, Dynamic Role-Based Policies, Delegated Administration, Auditing, and Standards. These areas are outlined below.

Multi Factor Authentication

VeriSoft Access Manager provides protection for the user's Identity with strong encryption (software and hardware) and with multifactor authentication. This allows the administrator to strengthen his security policies by requiring any (or a combination of) authentication method(s) for access to the system and associated services. All of these authentication methods are built into the system and work out of the box with supported hardware.

All user credentials are encrypted and stored in a corporate directory, and can also be made available for roaming users that require cached credentials (for access to identity information anytime while disconnected). Trusted Platform Module (TPM) user encryption is supported and once a TPM is initialized, user credentials are transparently encrypted and stored securely in the Directory. The TPM encryption option makes credentials available only to the authenticated owner of the credentials, therefore protecting user data from unauthorized access.

There are several Authentication methods built into the VeriSoft Access Manager. All provide additional levels of non-repudiation when trying to prove someone was the person performing a task or transaction (combined with the VeriSoft auditing subsystem). Below is an image of the Administration Center that lists some of the built-in authentication policies:

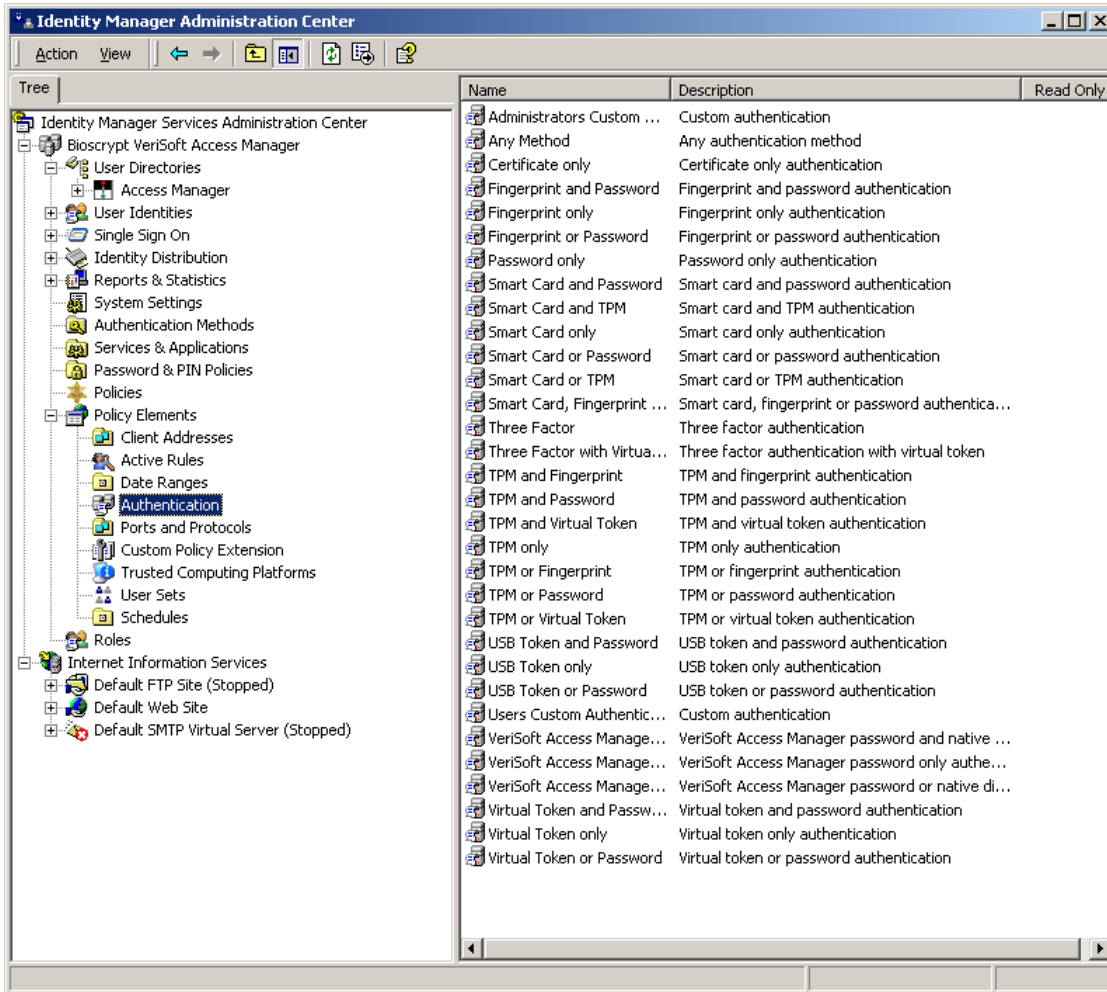


Figure 4 - Multifactor Authentication Options

Fingerprint Biometrics

The VeriSoft Access Manager has inherent support for best of breed fingerprint biometric technology. The Enrollment and Verification Wizards GUIs that are built into the client provide a consistent and easy to use interface for the end user, regardless of application.

The Bioscrypt fingerprint verification algorithm employs a unique and patented pattern-based approach to fingerprint comparison. The building blocks of this technique were originally developed by Arete Associates, a defense research company with over 25 years of experience in image processing, noise reduction, and pattern recognition associated with advanced sensor systems in use by the U.S. Department of Defense. This has resulted in a fast algorithm which has proven to be the most accurate and flexible in the industry. Most recently, it was awarded the most gold medals in the "open" category of the Fingerprint Verification Competition (FVC) 2004, a leading industry benchmark for fingerprint matching technology. (<http://bias.csr.unibo.it/fvc2004/results.asp>)

Bioscrypt's fingerprint comparison technique is performed in several steps. First, the fingerprint image is passed through a sophisticated image enhancement routine. Next, it estimates and removes the relative distortion between the candidate fingerprint and the (previously enrolled) template fingerprint. Finally, a correlation score is generated through a complex procedure which places a higher weighting on the less noisy and more content-rich areas of the print. This results in a high-confidence match with extremely low false acceptance and false rejection rates, even for users with more difficult fingers.

Fingerprints are the most widely used form of biometrics for the enterprise authentication space. Bioscrypt has been a leader in accuracy with the technology and leverages our history for best practices of fingerprint authentication within the VeriSoft Client.

Smartcards

VeriSoft Access Manager has the capability to support the inherent security capabilities of a smartcard within VeriSoft for authentication. Besides as a user authentication method, the administrator may configure and allow users to store their entire identity within a smartcard. This provides a distributed database for the user to have their credentials with them at all times regardless of network availability.

The VeriSoft Administration Center provides an interface for an administrator to issue and revoke smartcards for individuals. Management of smartcards can include the setting of policies to allow card personalization, PIN Management, and determining whether or not a card type is valid for authentication or simply credential storage. Smartcard removal policies can be applied which will log out the user or lock the user's workstation if configured by the administrator.

Certificates

A Public Key Certificate is a digitally signed document that is commonly used for authentication and secure exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority (CA) and can be issued for a user, a computer, or a service. This creates a trust relationship between two unknown entities.

VeriSoft Access Manager allows usage of these certificates for authentication as well as other digital signature and encryption in the enterprise. VeriSoft can handle certificates one of two ways:

1. VeriSoft can use a certificate stored on the PC or smartcard for authentication to the VeriSoft Access Manager.
2. VeriSoft can use another authentication method to log onto the Access Manager, but manage certificates centrally within the user's identity for distribution to any system they log into. VeriSoft can dynamically install and remove user certificates from any machine the end user logs onto.

Example: A Large bank wants to use Certificates for digital signing of data. Certificates are trusted for digital signatures and management is asking for their deployment. Most employees use multiple computers in their environment. The IT Manager knows that deploying a certificate solution for this environment can be a headache and has pushed back on upper management. Certificates typically reside only on the one computer they are installed on, or require a smartcard. VeriSoft overcomes that issue by allowing the Administrator to set a policy for users to allow their certificates to roam with them throughout the enterprise. The administrator simply requires another authentication method (such as fingerprint or password), and when a user logs into a workstation, his certificate is automatically transferred down from the server and installed on the workstation. When logging off of that workstation, the certificate is removed from that workstation.

VeriSoft's dynamic, roaming certificate support works regardless of Certificate Authority, and provides a simple way to ease the enterprise administrator's usage of Certificates.

Tokens

The USB Token, also known as a USB Key, contains a cryptographic chip for securely storing a user's personal ID. A USB Token is technologically identical to smartcards, with the exception of the interface to the computer. USB Smart Keys are about the size of a house key and are designed to interface with the universal standard bus (USB) ports found on millions of computers and peripheral devices. USB Tokens are becoming more and more popular as they fit onto a keychain and can essentially be with an end user at any time.

VeriSoft can support this token in the same method that it supports smart cards. The management interface is identical, and the user experience is the same – the only difference is the form factor. USB Tokens are an inexpensive and very portable additional security mechanism an administrator can require to improve authentication to the enterprise services.

Trusted Platform Modules

TPM hardware and software enhances the security of digital signatures, certificates, and the Encrypting File System by protecting the associated keys for these services.

Normally, in systems without the TPM, the keys used for these services are stored on the hard drive. Storing the keys on the hard drive makes the keys potentially vulnerable. In systems with a trusted platform module, the TPM's private Storage Root Keys, which never leave the TPM chip, are used to "wrap" or protect the keys desired by the services above. Breaking into the TPM to extract the private keys is much more difficult than hacking on the system's hard drive to obtain the keys.

The TPM also enhances the security of secure e-mail via S/MIME in Microsoft Outlook and Outlook Express. The TPM functions as a Cryptographic Service Provider (CSP). Keys and certificates are generated and/or supported by the TPM hardware, providing significantly greater security than software-only implementations.

VeriSoft has worked with Trusted Computing Group vendors to provide support of TPM modules that are within desktop and laptop computers available today. VeriSoft will attempt to identify the TPM within the system and if it is a supported TPM, the user can use the TPM for authentication and identity storage.

BioAPI Biometric Service Providers

The BioAPI Specification is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a Biometric Service Provider (BSP) to manage the Identification population for optimum performance. It also provides primitives that allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server.

VeriSoft provides the support for BioAPI BSPs and the installation and usage of these BSPs requires no development. The Administrator simply installs the appropriate BSP for the technology they are interested in using when installing the VeriSoft Client and Server. They simply select the associated BSP when configuring the BioAPI authentication method and it is now an available authentication option.

Example: A Government Agency has a requirement for the implementation of an Iris authentication system for logical access. The government agency will simply take the BSP from an Iris biometric organization such as Iridian and install that BSP and associated hardware on the desktops desiring that support. The administrator configures the BioAPI authentication method for Iridian's BSP and enables it for end users. Enrollment happens as part of desired policy and the iris templates will be stored at the server along with the rest of the user's identity.

Strong Passwords

VeriSoft does not require all of these advanced authentication methods to logon, and can require simply a strong password for authentication. Password Policies can be set differently for all components of the system (one policy for network logon, one for Single Sign-On automation, etc). The password options can be managed centrally, but include the ability to:

- Enforce Password History
- Require Minimum and Maximum Password Lengths
- Complex Password Requirements
 - # of Repetitive Characters allowed
 - # of Sequential Characters allowed
 - # of Duplicate Characters allowed
 - Check password against Dictionary

Directory Support

Almost every enterprise manages their users in some X.500 directory structure, whether an organization has Active Directory in house, eDirectory, or a combination of directories. Enterprise security problems start to arise when an organization has to make decisions on how to increase authentication and identity management across multiple directories.

VeriSoft Access Manager differentiates itself by having the ability to integrate into almost every enterprise directory available today with a simple wizard. With the proper directory identification and authorized credentials, VeriSoft has the ability to connect to that directory for direct read/writes of user data, as well as storage of additional user identity information. Once User Directories are within the system, VeriSoft can now assign rights to users in multiple directories by defining User Sets within the Administration Center.

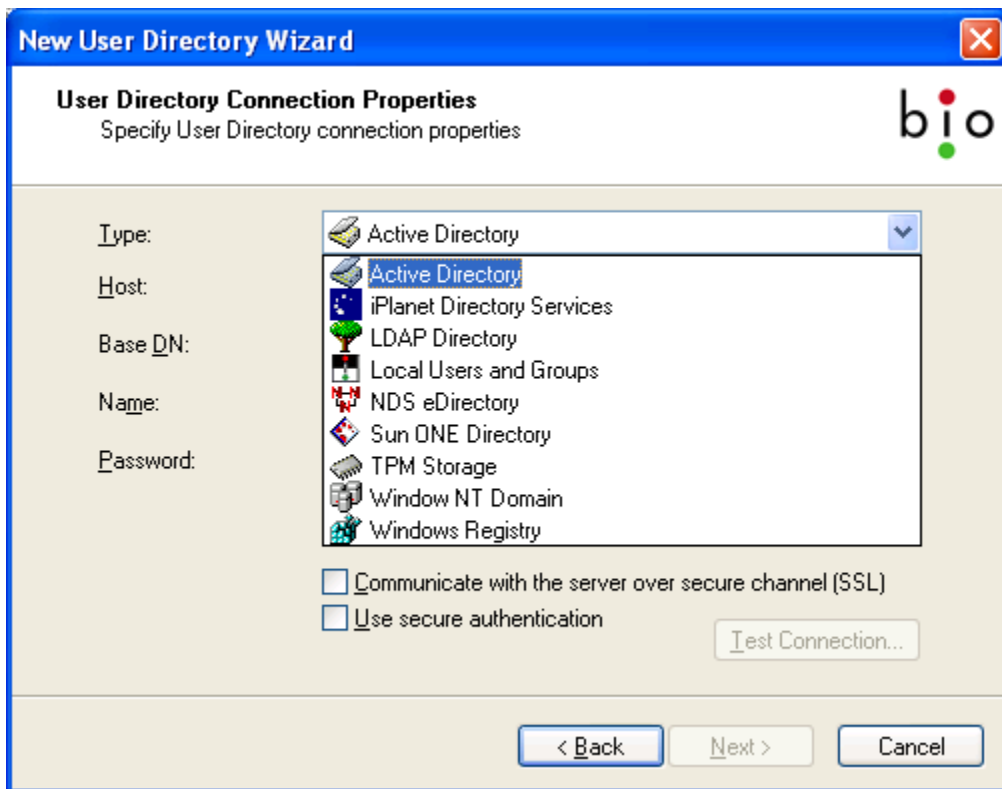


Figure 5 – New User Directory Wizard

Example: A Windows 2003-based organization has a collection of partners that they want to provide some application access that their internal employees also have access to. The IT Administrator does not want to put these external users into their Active Directory for several reasons, including licensing fees and potential security issues. With VeriSoft Access Manager, the IT Administrator can stand up an X.500 server separate from their Active Directory and manage users from both directories in one interface. He can then assign rights to certain applications based on User Sets which include users from multiple directories.

Communication and Encryption

The VeriSoft Access Manager Client communicates with the server through a communications channel using TCP/IP and HTTP/HTTPS protocols. VeriSoft was designed to allow for secure communications between the client and the server over port 80 as most enterprise firewalls will allow the communication between the client and the server without any special configuration.

Secure communication is available on four levels within VeriSoft Access Manager:

1. The client/server protocol is encrypted with a shared key. The administrator has the ability to define the Cryptographic Service Provider (CSP), cipher, and hash to be used for this key. This allows the flexibility that many security-focused IT directors require.
2. User data can be stored encrypted in the Directory. Again, the encryption is configurable by the administrator.
3. SSL link (HTTPS) can be used. Although all communication within the client/server protocol is encrypted, another layer of security could be added by securing the entire tunnel.
4. Secure authentication can be forced to any directory. The protocols used for directory access will be LDAP or LDAPS depending on the configuration of the administrator.

For remote sites where the VeriSoft server is not available from outside of the firewall, a Virtual Private Network (VPN) can be used and it is transparent to the client connecting to the server. With or without a VPN, if ports 80 or 443 are not the ports desired, the network administrator can change those ports on the VeriSoft clients and servers.

The communication to servers can be distributed and multiple servers can exist for one Master Repository of identity data. Clients can use DNS load balancing and other methods easily available to communicate with the servers available on the enterprise network.

Dynamic Role-Based Policies

Policy Management is one of the most complex components within the VeriSoft Access Manager. The tightly integrated framework allows for policies to be set using any bit of information to grant access to any component within the enterprise. The level of minutiae that VeriSoft Access Manager can get into when assigning rights to components of the system is the most powerful part of the application set.

Policy Definition

Within VeriSoft, a policy is derived from three components – Policy Elements, User Sets, and the User Role:

- Policy Elements are any component within the VeriSoft system. This can range from the IP Address of the machine(s), to the method(s) that a user authenticates with, to the Date/Time, to the ports and protocols that are being used at the time.
- User Sets are a collection of users in the directory(ies) or repository(ies). An administrator will define a user set that usually mirrors existing groups within the enterprise directories, and can directly call those groups as a User Set. User Sets allow you to combine users from multiple locations/groups/directories into one collection that you can logically manage.

-
- The Role is a logical representation of the user's role within the enterprise. This could range from anything such as an HR Admin, to a Finance User, etc. When the logical roles have been thought out within your organization, the Administrator simply adds them to the list of roles within VeriSoft.

The successful application of a user's Role happens when all of the required policy elements occur for the user who is contained in the specific User Set. To begin defining VeriSoft Access Manager policies, the first step is to determine a logical role within your enterprise. Once that is defined, you can create policies to define what is required to give someone that role.

Examples

Example #1: An Enterprise wants to ensure that only those individuals that authenticate with a fingerprint have access to the Single Sign-On component. Without Single Sign-On, end users do not know their passwords that have been managed on the back side and cannot log into their applications. The Administrator can create a role for a SSO User (Single Sign-On User) and define the required elements and user set. The administrator requires that 'All Users' in his enterprise who Sign-On with 'Fingerprint Only' will get access to Single Sign-On. He completes the policy and applies that directly to the Single Sign-On application. End users who log on with only a password now will not have access to their applications.

Example #2: An Enterprise has HR Administrators that they want to add the ability to manage users at a minimal level. All the IT department wants HR to do is add users and register fingerprints. An HR Admin role is defined as anyone in the HR Admin group in Active Directory. The Administrator simply creates an HR Admin Role within VeriSoft and adds the HR Admin User Set to that policy. The Administrator applies this role to the Delegated Administration service and turns off all options except for creating new users and enrolling fingerprints. The HR Admins now have access to the administrative console but only two very small components that are needed to complete their job function. (More of this will be discussed in the next section.)

Delegated Administration

In order to manage security throughout the enterprise, there are often different levels of people that should have access to multiple parts of the enterprise systems. Some individuals will be required to enroll fingerprints for people, some will create users, and some will manage certain applications. VeriSoft Access Manager has a very flexible and robust Delegated Administration capability where any component of any application can be enabled or disabled based on the user's Role.

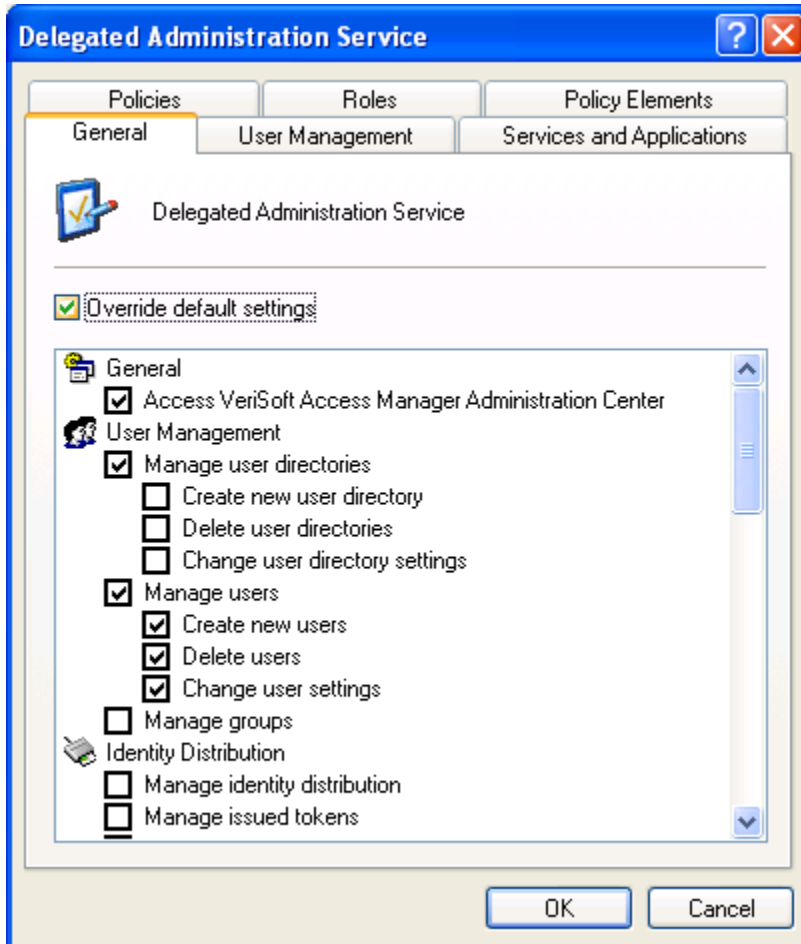


Figure 6 – Delegated Administration Service

With the support of the flexible policies, any part of the management of the system can be enabled or disabled based on enterprise needs. The above image is for a particular role that only needs a certain subset of features available.

Auditing

One of the most important components of any enterprise security solution is the ability to provide an audit trail that can be viewed at any time to identify what happened within the enterprise and who, where, when, how and why it happened. The VeriSoft Access Manager provides multiple levels of auditing and reporting available to administrators based on any information they require.

The VeriSoft Access Manager uses a Windows Event Viewer style auditing log which can be accessed by any Administration Console. The administrator has the ability to browse the entire log, or perform ad hoc queries at any time on any piece of data within the database and save these queries for future use and reporting.

VeriSoft's query engine is based on SQL query technology, providing administrators similar query capabilities to those they are currently using throughout other parts of their enterprise. The administrator has the ability to perform a query of any combination of information from any part of the audit log, using either an AND or an OR relationship between the data elements. This provides the scalability and personalization of reporting that is needed throughout the enterprise.

Example: The administrator has a clinical workstation in his hospital, but does not use enterprise network logon as the workstation can always be logged in with a guest account. This clinical workstation is used to perform prescription filling for the hospital's pharmacy and the administrator needs to do a quick look at who has been accessing the computer. The administrator simply puts a query together that asks for all Logon/Logoff events for this particular workstation. Because this workstation is the only workstation available for this task, the Administrator now has a saved query he can use anytime to determine who has been accessing that machine. One mouse click and he sees an updated real-time query of the requested data.

Standards

The VeriSoft Access Manager and the products contained within have been developed under strict guideline of industry standards and it is fully compliant with the following standards:

- HTTP/HTTPS
- XML
- AES
- 3DES
- BioAPI
- DCE
- GSS-API
- LDAP
- RPC
- TACACS+
- X.509
- PKCS#11

For More Information

Please contact Bioscrypt @ <http://www.bioscrypt.com>