A BIO-key® Solution.

White Paper

Active Directory and Identity Management

Table of Contents

Table of Contents

White Paper Summary

Secret codes, passwords, security phrases – these are all modern names for a much more archaic practice. As far back as the Ancient Egyptians, codes and various secrets were in place to deter anyone from obtaining specific information unless they were already in the know. It is a testament to the complexity of human nature that secrecy and security has been such a staple in our culture over so vast a time.

In the modern age, passwords, security questions, shared secrets – these are all aspects of identity management. Our numbers have increased since ancient times, and the rise of the digital era has required an evolution in both identity management and access control. The chief player at the center of this evolution is none other than Microsoft Active Directory.

In this paper you will learn why Active Directory is effective at identity management and why so many organizations still make use of it as their Central User Repository. Whether you are looking to stay locally, on-premises or journey into the Cloud – Active Directory will serve you well, and PortalGuard can help.

Authentication Past and Present | Secret Codes and Passwords

Where We Began

In 14th Century England, entering a private or protected place might have been possible through a pre-determined code of knocks on the door, or a code word used by any individual attempting to gain access. This code, or 'password', might change on occasion, but usually only after it fell into the wrong hands. Authentication was also achieved by other means, such as requiring entrants to produce a letter with a wax seal of their kingdom or lord.

There was no need to keep a dedicated record of the individuals who knew the secret in order to validating their identity and right to gain access – that one shared secret was proof enough. Meeting places changed, ciphers were created, but proof of one's identity was relatively simple and trusted.

Throughout the course of history, symbols, words, phrases, keys, and secret codes have been assigned to individuals and groups to authenticate and gain access to a large array of places. From castles, fortresses, and hideaways, to rebel meetings and private organizations - the uses for a shared secret were vast. Then the digital age arose and the uses for a shared secret became nearly boundless.

Authentication Today Identity Management

Fast-forward to the present and, with the proliferation of computers and networks, access is still primarily granted through the use of passwords. While the notion of a shared secret or a password has remained, the security of that secret has changed drastically. Although passwords and codes have become unique to each individual, they can still be lost or forgotten – making them less secure than one might hope, and leading to a rise in demand for stronger security and authentication. [i]

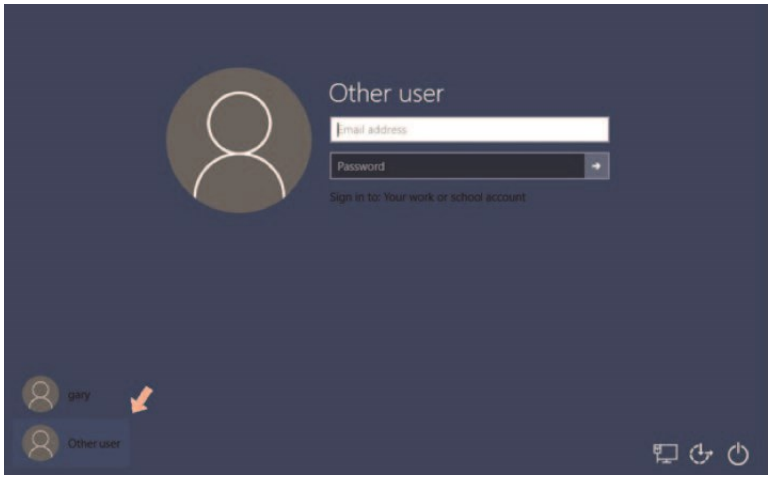
Now that organizations possess numerous web applications, and a continually growing repertoire of cloud applications are being added each and every day, the need to address the growing complexity and frustration of identity management is at an all-time high. Knowing the secret is no longer proof of identity – it is no longer enough to grant you access to the secret meeting. Private and corporate information is too verbose, and far too valuable to be secured by something so simple. Unfortunately, it is the individual who pays the price for this increase in security.

"Before PortalGuard, our students had several passwords to remember. With PortalGuard, they only have one password, and if they forget it, they can reset it on their own."

- Andy Clermont Northeastern Schools

However, despite popular belief, the future may not necessarily see the death of the password or 'secret code' – especially with new strides in Single Sign-On technology being made to reduce password related stress and fatigue. SSO allows for the user to access all apps by authenticating once to a central, trusted authority using a single secret code:

The Active Directory password.

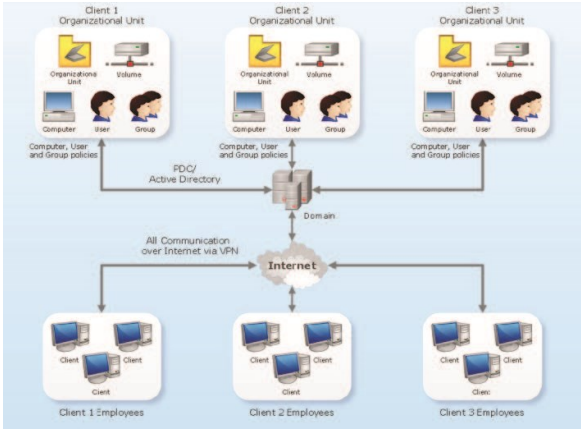


A Central Directory For Identity and Access Management

Authentication against a central directory such as Active Directory harkens back to the days of yore by allowing end-users to use and remember only one password. Only a single secret is required to be recalled or changed while still remaining secure and vigilant in accessing and protecting information that is both private and valuable. This validation against Active Directory eliminates downtime and boosts productivity – the direct opposites of which are related to password fatigue and associated issues.[ii]

Active Directory As a User Repository

So why do so many organizations choose Active Directory for their go-to user repository? The primary reason is because it was designed specifically for this purpose. Active Directory sets up a logical hierarchy from each individual object (users, printers, computers, etc.) through to an over-arching Global Catalog for the entire enterprise/ organization. The setup allows for simple and easy administration and access management. Put quite frankly – Active Directory simplifies identity management into a well-organized and easily searchable hierarchy.



In the world of IT, where it is too easy for things to become complicated, simplicity is king. Complexity leads to issues, which lead to more overhead, data breaches, etc. With a simple, easy to navigate user database, troubleshooting and organization become substantially easier to manage. For those organizations that want a more custom or specific method of organization, Active Directory promotes usability on the administrator side as well – allowing complete hierarchical configuration over Domain Structure and object organization. This functionality makes it perfect for the Tinkerer and the Troubleshooter both – and it plays well with others.

A Nondisciminatory User Repository For Mac and Windows

Cross-platform functionality is a must in the current digital climate. While Windows easily has the largest market share at the moment, the fact of the matter is this – users will be working on both Windows and Mac operating systems. That is the truth of the digital world, as it exists today.[iii]

The struggles that this multi-platform landscape engenders are real, and they often create problems in corporate infrastructure when there is not a single method of proving and managing user identity.

Luckily, Active Directory is built to handle and support an environment that sees extensive use of both Windows and Macintosh OS X.

Windows and AD

Microsoft Active Directory works inherently with the Microsoft Windows suite of Operating Systems, ever since the development and release of Windows 2000. With the simplicity inherent in the existing hierarchy, Active Directory is an obvious solution for organizations of any size, in virtually any business vector. Even personal networks may find Active Directory as a viable choice, simply for the many doors that may be opened when AD is at the heart.

Notably, Active Directory has built-in support for the Kerberos authentication protocol (for more information see our **Kerberos** section below). This allows for a wide array of Single Sign-On and secure access control methods right out of the box.

For networks of any size, Active Directory has an answer.

To add a Windows Machine to your Active Directory Domain Controller, you need three (3) main things:

1. Knowledge of the appropriate DNS settings to point to the Domain
2. Administrator credentials for the Active Directory Domain.
3. A recognizable Machine name.

"The struggles that this multi-platform landscape engenders are real..."

For more detailed instructions on adding a Windows machine to the Active Directory Domain, see Appendix 1.

Once the machine has been appropriately joined to the Active Directory domain, configuration for login type may be adjusted as necessary for your environment. Login methods that can be configured natively in windows include changing the login type to show a list of users, to specifically request a username and password, or even through other services like the use of a Smart Card.[iv]

Macintosh and AD

It's no secret that Apple has their own unique way of doing things – far afield from the typical processes that many users with Windows machines are accustomed to. For authentication and identity management, Apple even developed and implements its own User Repository - termed Open Directory (OD). However, that does not mean that an environment has to implement both AD and OD, nor should it shun users of the various Mac operating systems when a much simpler solution is available.

Mac OS X has out-of-the-box support for a variety of directory-service technologies, including Active Directory.

MacOS X uses Kerberos as its default authentication, much the same as Windows 2000 and up. With this protocol in place, Mac OS X is primed and inherently capable of supporting many beneficial Active Directory functions, such as password policies, restrictions and enforcement. A simple to manage configuration within the Mac preferences will allow you to 'Bind' the machine to the Directory and configure the necessary Domain components from there. For more information on managing this configuration, **see Appendix 1, Section B.**

Mac System Keychain

As any Mac user will know, Mac OS X has a somewhat unique manner of handling multiple passwords – the keychain. OS X creates a unique keychain for each individual user, as well as the machine, and encrypts passwords therein. In order to access the contents of the keychain, you need the appropriate master password.

As many users of both Mac and Windows machines have undoubtedly found – this functionality is not without its own curses and bumps in the road.

When a Mac machine is bound to an Active Directory domain, the machine creates a unique system password and saves it to the System Keychain for validation against Active Directory whenever a user logs in. By default, the Mac sets the expiration of this Keychain Password to 14-days, but it can be configured by use of the dsconfigad Terminal commands. For specifics, see **Appendix 2 – dsconfigad Terminal Commands.**

Important Note: The System Keychain is different from the Login Keychain, which is unique to each individual user account.

The Login Keychain acts as a secure storage vault for additional user passwords. Upon first login to the bound Macintosh machine, the Login Keychain will be created and the Password will be synchronized with the set Active Directory password.

For Macintosh users, the Active Directory password must be changed, prior to its expiration, within the ***Users & Groups*** section of ***System Preferences***. In this manner, the OS automatically updates the Keychain credentials without any additional effort on behalf of the user.

One of the drawbacks to the Mac Keychain is the likelihood of forgetting your Keychain master password, or resetting the Active Directory password on another machine/in another location. If either of these events were to occur – the user would typically be required to create a new keychain and destroy the existing one.

One of the capabilities of proper integration with Active Directory is the use of password recovery to retrieve the forgotten/changed password in order to update it on the machine.[v] This route requires an extra step on behalf of the end user, but prevents loss of any important/necessary credentials.

OS X Desktop Password Reset

Desktop password reset is nothing new for Windows users – simply use the ***CTRL + ALT + DEL*** key combination to open up a window, which enables you to change your password as needed. It's quite simple, but a feature that does not exist within Macintosh OS X by default. As noted above – the appropriate (and necessary) method of natively resetting your password in OS X is through the ***System & Users*** section of the ***System Preferences***. In addition to synchronizing the Login Keychain, this process also updates the password directly in Active Directory – prepping the account for access in all other locations using the new credentials

Another lacking feature in the native Active Directory setup, however, is that there is no way to reset a forgotten Active Directory password at the login screen of a Macintosh machine.

Fortunately, Active Directory Identity Management solutions do exist that will enable password recovery and Self-Service Password Reset directly from the Mac login screen to prevent any decrease in productivity and progress.

Mobile Access

Mobile use is not only popular among many users today – it is an expected reality. With the mobile takeover hitting the digital realm in recent years, an ever-increasing number of users are entering the workplace with a wirelessly accessible smartphone. If employees are receptive to using their personal devices for work purposes, why not make use of those devices for identity verification? It is a simple and cost-effective solution for accessing and implementing other authentication security measures such as Two-Factor tokens.

Apps and Active Directory

Typically, mobile apps do not authenticate directly with Active Directory – or any other local user repository. Most mobile apps reference a third party—To use Office 365 on mobile, for example, you validate to Office by default, not your local directory. However, there is the possibility to federate directly with on-premises Active Directory domains.

Due to the standards-based nature of Active Directory, applications such as the PortalGuard Self-Service Password Reset App (Available on ***iTunes*** and ***Google Play***) are able to allow users to reset their local Active Directory password directly from their smart phone device.

Additional Devices

On top of everything else, Active Directory can be configured to communicate with devices other than computers and printers, such as tablets, smartphones, e-readers, etc. Both businesses and educational industries have seen the rise of various BYOD programs,[vi] and Active Directory has the customizability to provide accurate identity management across multiple operating systems and devices.

Consolidating Passwords
Reducing Password Prompts

Password fatigue is a common issue, even if you don't often see it directly. It has become common practice to save passwords within browsers, but the annoyance and frustration of clicking through each individual login screen is still there – and steadily increasing. Password fatigue and related issues can pockmark productivity and bring individual progress to a grinding halt.

For the 14th Century Englishman or Englishwoman, there was no escaping the frustration of having multiple shared secrets. A well-known seal could prove who you were, but not if you belonged, and so a wide variety of passphrases and shared secrets were necessary. Authentication may have been relatively simple – but it was still incredibly verbose at times.

With Active Directory Single Sign-On, the modern age has the capability to eliminate this issue in a simple and secure manner using various industry standards – a critical necessity for both usability and compliance. For more information, see the **Compliance** section below.

Kerberos

Named after the mythological three-headed guardian of Hades, the Greek underworld, Kerberos is an authentication protocol that relies on mutual authentication and a trusted third-party. Kerberos was built and designed at the Massachusetts Institute of Technology as an additional method of securing network services provided by ***Project Athena***.

As the referential name would imply – Kerberos implements a three-part authentication process that builds on symmetric key cryptography. The three 'heads' of Kerberos Authentication refer to the Key Distribution Center (KDC), the client machine and the service provider. The KDC can be installed as part of the Active Directory Domain Controller (DC) – introducing the trusted third party into mix.

The basic process of Kerberos proceeds as follows:

1. Client Machine Creates Ticket Granting Ticket (TGT) for User†
2. User attempts to access a Service Provider
3. Client Machine receives a Session Ticket from Domain Controller and submits it to the Service Provider††
4. Service Provider validates the Session Ticket and returns a new Session Ticket to the Client Machine
5. The Client Machine submits new Session Ticket to Domain Controller for validation
6. User is Granted Access to the Service

This entire process - from start to finish – happens rapidly behind the scenes. If Active Directory and the service in question are appropriately configured for Kerberos Authentication, the user need only make the initial request and the service will be provided without any interruption.

†The TGT is only updated upon login or through a change in the password in Active Directory, and enables Kerberos Authentication for the duration of the login session.

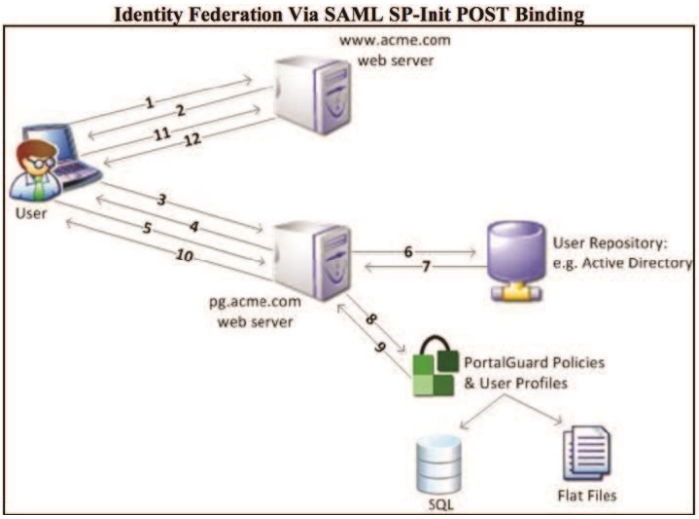
††The Session Ticket contains a User Identifier, minus password, alongside an encrypted shared-secret for the SP to decrypt.

Security Assertion Markup Language

SAML is an open-standard authentication protocol, which enables user authentication between an Identity Provider (IdP) and a Service Provider (SP). A SAML Token containing user-specific attributes is created by the IdP and automatically sent to the SP in order to validate a user without having to repeatedly login via traditional methods.

By using an IdP such as PortalGuard in conjunction with Active Directory and SAML, Single Sign-On can be achieved without any downside to the individual user. No confidential information is shared – the login credentials are not transmitted directly to any of the target websites – and the Service Provider is able to validate the authenticity of the SAML Token directly, in order to provide secure authentication.

Most Identity Providers can easily utilize Active Directory to provide out-of-the-box SAML SSO to literally thousands of on-premises and cloud-based websites.



Central Authentication Service (CAS)

Shawn Bayern at the Yale University of Technology and Planning developed the Central Authentication Service (CAS) primarily for Single Sign-On, but it later introduced multi-tier proxy authentication. Since its inception, and throughout its various versions that exist today, much the same process for SSO authentication has occurred. CAS uses a three-party approach similar to Kerberos for authentication – with a specific requirement of a dedicated CAS server.

For more environments that require more direct authentication management than is provided through standards such as SAML, the CAS protocol can be configured for many web applications. While the structure of CAS may be reminiscent of Kerberos, the process itself is more akin to that of SAML SSO. Much like using SAML, CAS enables Single Sign-On to a preconfigured list of web apps by providing two-part authentication. When the web app in question requests validation, it communicates with the CAS server and not the user, at which point the CAS server provides a service identifier and a security ticket to be verified by the application.

As with other SSO methods, this process happens behind the scenes and will not require the user to provide additional credentials unless the application has not been configured for Single Sign-On. Additionally, no security credentials are put at risk because they are not transmitted to the web application directly. Given its wide-ranging support for various web applications, the CAS protocol is often used heavily in the education vertical. [vii]

Leveraging Existing AD

Most business or educational institutions already employ Active Directory for Windows login – opening the door to the possibility of reduced or Single Sign-On to an expanded assortment of web applications through any of the above protocols.

Using Active Directory as a user repository for identity management, as well as an anchor for Single Sign-On will reduce the threat of an intruder gaining access due to an improperly crafted or stored user password. When the end-user is only required to remember a single secret code, they are much more likely to accept that reality and reduce the likelihood of compromising security.

Password Issues
The Daily Confrontation

Password complexity is a key component in maintaining a robust security policy. The evolution of the microchip has improved every aspect of modern technology – including the Hacker's ability to crack passwords. Increased processing power has transformed life for a hacker in the modern age - what once would have taken days or weeks to accomplish, can now be done in minutes or hours. [viii]

Guessed and cracked passwords are still among the most common threats to corporate security (accounting for nearly 25% of all network attacks). With users having an average of 25 online accounts that require passwords to access – password strength and security is often sacrificed for an increase in convenience.[ix] This sacrifice opens the doors for simple password cracking and puts a wide array of sensitive data at risk of exposure. If the ***2014 Year of Data Breaches*** has taught the world anything, it is that one thing remains the same between the 14th century and today: money and finances can be replaced, but your identity is much more difficult to recover.

In an effort to avoid these losses, and to increase protection against the more sophisticated attacker, there has been a strong transition towards a more secure and complex password in order to protect user information - a move that has been met with much trepidation. With the various password complexity and strength requirements set by the ever-increasing number of password policies that users must adhere to, the frustration and confusion surrounding what makes a password 'strong' is overwhelming. In the corporate setting, this requires educating end users on proper complexity and password policy adherence – a tremendous time sink for any organization.

Bit Complexity

Password Entropy

Entropy is a measure of password strength calculated from length and complexity. Entropy is the measure of uncertainty (eg. Difficulty) a password has, and is typically represented through bits.

The two tables below illustrate typical bit amounts and the difficulty each value represents for standard cracking methods. NOTE: common words/phrases, while possibly high in entropy, are incredibly weak against attacks using Rainbow Tables or the like, making them much less secure.

	Complexity		
Password Length	Numbers 0-9	a-z	a-z, A-Z, 0-9
8	26 bits	37 bits	47 bits
10	33 bits	47 bits	59 bits
11	36 bits	51 bits	65 bits
12	39 bits	56 bits	71 bits
13	43 bits	61 bits	77 bits
14	46 bits	65 bits	80 bits
15	49 bits	70 bits	89 bits
20	66 bits	94 bits	119 bits

Entropy	*Maximum Time to crack @ 350 Billion guesses/Sec*
47 bits	0.223 Hours
59 bits	457.50 Hours
65 bits	3.342 Years
71 bits	213.92 Years
77 bits	13,690 Years
80 bits	109,527.95 Years
89 bits	56078315.93 Years
119 bits	6.0213633 e+16 Years

Some organizations may allow this issue to fall by the wayside – unwilling to put in the time, and confident that the risks are without warrant – doing so puts the livelihood and reputation of a company in harm's way. Without implementing a better regime for understanding and adhering to appropriate password policies, companies and various organizations could be putting themselves at risk for proper compliance or governmental regulation adherence (See **Compliance** section below).

Caution!

Weak Admin Passwords

Administrators' passwords can often be weak and thus easily seized by potential intruders or hackers - granting unhindered access to systems and sensitive information.

Both end-users and administrators sometimes share their passwords with co-workers and friends, ultimately compromising security by enabling those passwords to potentially end up in the hands of an unauthorized person.

Be requiring administrators to enact a password reset, organizations are allowing for the potential of one or more individuals knowing, or having access to, the passwords to multiple user accounts.

Enforcing strong password policies is a strong step towards eliminating this weakness before it has the opportunity to threaten your organization or your information.

With Active Directory integration, these password-related issues can be reduced to almost nothing. Use of various Single Sign-On protocols that are compatible with Active Directory will reduce the strain of remembering and retaining a high multitude of strong passwords with varying complexities.

Active Directory Single Sign-On gives an organization and its users a strong level of security with a high level of convenience – one that is strictly and completely configurable within the confines of Active Directory.

Active Directory
Password Reset

What happens when your shared secret is changed, and you cannot be informed of this fact before your secret, shadowy affair is set to take place. There was a time when you would be turned away simply for not having the updated information – and there was very little that you could do about it.

With the implementation of Active Directory as a central user repository comes the ability to enable various methods of Self-Service Password Reset – enabling the ability to adjust or alter your secret on an as-needed basis.

Even when users need only recall a single, heavily secure password, it is still likely that the password will be forgotten on occasion. In these instances, system lockouts and other difficulties can tie up a helpdesk, keeping production on other important tasks from being accomplished, or worse - introduce various additional security concerns into the environment.

The most commonly used work-around to a system lockout is for an end user to either call the helpdesk or login to a guest account on a different machine. Not only do both of these options impede productivity, but the latter method also disrupts an additional workstation and can potentially introduce a publicly accessible/weak point into the digital environment.

Fortunately, Active Directory integration provides an answer for these concerns and much more by opening up the door to provide an end user with the ability to reset their password without going out of their way. With proper Active Directory integration, many different methods to unlock a user account become available – all without having to call the helpdesk for administrative support.

Mobile Methods

Linking Active Directory with a dedicated Identity provider enables various methods of One-time Password (OTP) delivery. In the early days of Multi-Factor Authentication (MFA), one of the most common methods of delivering an OTP without the use of a Hardware Token had initially been via e-mail. With the advent of the mobile era and BYOD programs, OTP delivery has taken a whole new face.

SMS OTP Delivery

An IdP can be configured to send an OTP to SMS for free via open standard SMS gateway protocols. By using this method, users can enact a password reset quickly and securely by making use of their cellular network connection.

Mobile App Password Rest

An additional option for Active Directory Password Reset is through using a mobile application. With mobile access, certain IdPs allow for one-touch password reset that updates Active Directory instantaneously over the network.

Challenge Question Validation

Knowledge-Based Authentication (KBA) is a form of authentication that relies on specific knowledge from the user. The most common version of KBA is the static form – use of preconfigured challenge questions for the user to answer in order to prove identity. By synchronizing Active Directory behind a series of unique, customizable challenge questions, password reset can be handled securely from any network-connected device.

Dynamic KBA can also be synchronized with Active Directory. Through Dynamic KBA, challenge questions are generated on the fly from information stored in the user profile.
This information can be very specific to the user or very generic, depending on configuration.

OTP Verification for SSPR

Much like the mobile systems for authentication, various other methods of OTP delivery are available to users for password reset validation. As a prime example, PortalGuard offers support for eleven different OTP methods, ranging from Hard Token to completely token-free support.

Offering various methods of securing and validating a user account provides convenience to the user without impacting productivity and usability. Active Directory configuration allows for multiple validation pathways that enable the user to access his or her account without going through the helpdesk.

These multiple pathways can only be accessed by the user in question – and must be preconfigured beforehand. As such, the user receives the convenience of choice while still retaining a secure method of authentication that prevents hackers from getting into the network.

Windows Desktop Password Reset/Recovery

Password Reset

Active Directory natively integrates with Windows operating systems. Through this integration, password reset is enables via a desktop hotkey shortcut – **CTRL + ALT + DEL.** Simple as it is, however, this default integration only enables for password reset if the user knows the current password.

This method of Password Reset is perfect when paired with password expiration notifications, as it offers a simple method for users to update their password in accordance with company/local password policy requirements.

Password Recovery

For instances where a user has forgotten his or her password but has not lost it, or otherwise simply needs to recover the current password, basic active directory configuration will only serve as a foundation.

Through the use of an adequate IdP, the end user can validate via different methods – such as OTP or challenge questions – and then either retrieve or reset the Active Directory password straight from the desktop.

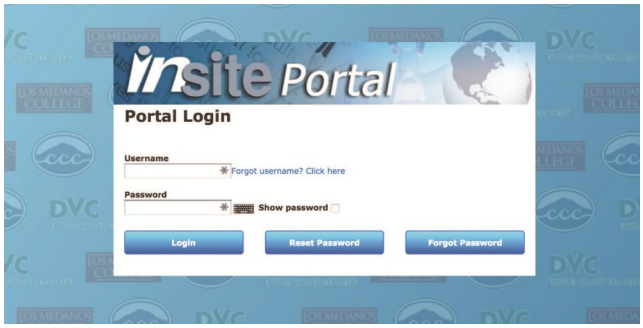
For the more information on this functionality on Mac OS X, please see the Macintosh and AD section above.

Web Portal

Active Directory can also be integrated with your existing web portal in order to provide an additional method of password reset for situations where Desktop or mobile password reset are inaccessible. In these situations, a web-based active directory password reset will remove the need for a user to contact the helpdesk for access to the portal.

Custom User Interface

Some IdPs will enable you to brand a Custom web-portal in order to provide web-based password reset without confusing or alienating your existing users. PortalGuard goes one step further by providing basic functionality for a brandable UI to remain consistent with the rest of your existing website.



PortalGuard SideCar

For organizations with an existing web portal who still wish to enable web-based Active Directory Password Reset, PortalGuard has SideCar. SideCar enables web-based password reset through the use of a dedicated IFRAME. This windows provides access to Self-Service Password Reset without leaving the existing web-portal or having to call the helpdesk.

Looking for More info?

Visit the PortalGuard Resource Center

AD Password Reset and SSO
The Benefits

A Single Password Policy

Built directly into Active Directory is the ability to modify password policies and password complexity requirements at the Domain, Group and User levels.

By implementing Single Sign-On with Active Directory, an organization can then implement a single strong password policy instead of requiring end users to manage several different policies. That is like standardizing the secret codes for every late-night rendezvous met by candlelight – simplicity is offered and security does not have to be compromised.

Additionally, AD SSO integration creates a simple password reset procedure by necessitating only one password change that affects all synchronized accounts. This set-up improves usability and convenience for end users while also reducing the number of calls made to the helpdesk for password resets or related issues.

Password Policy Features that May be Set in AD[x]

- Password History
- Password Age
  - Minimum
  - Maximum
- Password Length
  - Minimum
  - Maximum
- Password Complexity
  - Character Requirements
    - Uppercase, Lowercase, Base Digits, Special Characters, Other Unicode Characters

Password Policy Best Practices[xi]

Typical password policy best practices are to set "Passwords must meet complexity requirements" in Active Directory, as well as the following:

- Minimum Password Length of 8 Characters
- Use of ALT key characters for Administrators and similar Users/Groups
- Use of at least one (1) special character
- Require the password to be different from the username/display name
- Blacklist dictionary words

Two-Factor Authentication

Strengthening the Front Door Password Reset

Adopting a solution that integrates with Active Directory and provides SSPR and/or SSO is a major boon to the security of any given environment. By relegating all password-related structure and configuration to the main AD password, an organization can strengthen the front door to the network much more than it would be able to strengthen each individual login.[xii]

Specifically speaking, end users are far more likely recall and adhere to a single set of strong password policy requirements. This condenses security risks inherent with implementing various accounts with additional passwords that lead into various locations within the network. Moreover, Active Directory has native support for solutions to pair KBA and OTP delivery for augmented authentication security.

Proper implementation turns a single point of failure into a strong and heavily fortified single point of access that can be easily monitored and defended in the event of a stolen password or similar.

Two-Factor Tokens

While we have discussed the uses of Two-Factor Authentication in Self-Service Password Reset, as well as the various methods of delivering an OTP via a second factor, this additional layer of authentication exponentially increases the strength of a login when paired with Single Sign-On.

Most existing Two-factor Authentication token providers have support for Active Directory built in – which makes adding that additional physical factor a much simpler feat to accomplish when Active Directory is the central user repository in a given environment. This makes sense for various situations, including those environments where compliance adherence is a must.

Cloud and On-Premises

The Rising Trend

More often than not in the current age, many institutions are making the transition to the cloud.[xiii] There are a host of both advantages and disadvantages to making this jump – and the primary environment in question is a large factor in making this decision.

The major benefit to making the shift to cloud hosting for web applications and services is the ability to easily expand existing IT infrastructure, or add an entirely new variation of that infrastructure. Despite this benefit, price can often turn into a major issue when determining true return on investment.

Some additional questions to consider when looking at a Cloud-based solution for Identity and Service Management are the location of the user database, the security therein, and how each method will affect local or government compliance requirements. (Sidebar quote?)

Where are my Users Stored?

No matter the local environment – there needs to be a user repository for authentication and identity management. Making the choice to use Active Directory provides various options for implementing this database in systems that might integrate Cloud-computing in full or just as part of the existing environment.

Local

Local Active Directory database storage comes with a dedicated hardware and maintenance cost – but this also allows for another level of security. While local, on premises hosting of Active Directory puts the upkeep and service costs in-house, this method also enables a higher level of access control and security to be implemented by the owner of the directory.

Additionally, a specific compliance may require that a user repository be hosted locally as opposed to a cloud. Active Directory allows for flexibility in that regard.

Azure AD

Microsoft Azure Active Directory is the cloud-based iteration of Active Directory. This model hosts the entire directory in a multi-tenant, cloud-based directory for identity and access management.[xiv] Hosting the directory in this manner allows for simple, easy integration with existing SaaS applications and services – Microsoft or otherwise.

Much like the locally hosted Active Directory, Azure AD also features support for SSO and 2FA functionality.

The Hybrid Approach

If various aspects of both the cloud-based and on premises approach to Active Directory and Identity Management seem to be worth considering – Active Directory also lends itself to a Hybrid approach. There are two common variations of a Hybrid hosting situation: Active Directory hosted Locally with Access Control to cloud apps, or hosting a private cloud.

Locally Hosted AD with Cloud App Integration

This method allows an organization to retain the security and compliance requirements met by hosting user data and login information on dedicated, local servers while benefiting from the convenience and cost-savings of hosting all applications in the cloud. A cloud-based Identity Provider can then access Active Directory using a secure network connection/tunnel before providing users with access to the applications that are hosted elsewhere.

Private Cloud

Hosting a private cloud with Active Directory on a dedicated server is another way to go. This method is not as far ranging as true cloud computing, but enables certain organizations to maintain the security of knowing exactly where user information is stored. For auditing and compliance purposes – this added security and convenience serves as a plausible alternative to trusting the entirety of their user data to an unseen location with minimal transparency about replication and access limitations.

Compliance

Everything in the modern age is regulated by something else. Federal governments regulate local Governments, and those regulations often get passed on to organizations in order to dictate the security and safety with which they operate. Additionally, some organizations are regulated by the needs and expectations of their own customer-base.

Gone are the days where only a King, or a Queen, or possibly a local Lord could impose stringent rules and regulations on the goings on of your daily life. Today – compliance is a necessity and offers an entirely new level of security and peace of mind for businesses and individuals alike.

Internal
Corporate Compliance

Various corporate vectors rely on strict compliance adherence for customer relations, as well as corporate policy and procedure. Requiring and implementing a compliance policy of this sort is one matter, while enforcing it is another issue on its own.

Depending on the particular organization, Active Directory may provide access to the capability for better enforcement of local, internal compliance. Making use of the previously mentioned auditing and authentication features available out-of-the-box in Active Directory is one method of accomplishing this without having to reach out to third-party providers.

Where confidentiality or access control is required by such relationships, Active Directory has the capability to address these concerns securely, while assuring end-user compliance as a matter of course. It is for this reason that Active Directory is also a top choice for user repository in situations where adherence to governmental regulations and compliance is concerned as well.

Regulatory Compliance
Entails Securing Critical Data

Compliance with governmental regulations has not only been a hot issue for corporate management, but a major concern of IT departments as well. These regulations mandate that organizations protect and secure access to sensitive financial data as well as customer and patient information, which dramatically impacts the IT infrastructure and the overall business processes.

In the past decade, several laws have been passed that have forced organizations to establish corporate compliance policies. The three most significant laws are: the Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLB).[xv]

As organizations coordinate their response to the recent governmental regulations and begin implementing the necessary changes, there are many IT solutions that should be considered. However, password management is one of the most instrumental factors in maintaining secure access control for protected information. Thus, password management should be a significant portion of any organization's compliance strategy.

Government Regulation
Requirements

There is a significant overlap in the requirements raised by the main corporate governance and privacy regulations, as outlined below. Common requirements that are satisfied by password management capabilities are:

1. Strong and reliable authentication
2. Strict control over end-user access to systems and data, including timely removal of access after an employee departure
3. Thorough audit trails and reporting on end-user access to specific systems and data

The PCI DSS
Compliance Big Hitter

A relatively recent addition to the realm of compliance is the Payment Card Industry Data Security Standard – the PCI DSS.[xvi] Initially looked at as a compliance requirement purely for retail and online shopping, the PCI DSS is a major concern for any organization or business that handles credit card transactions for a variety of reasons.

The PCI DSS exists primarily to ensure that the technology within a given environment is sufficient enough to protect the customer from data/identity theft, as well as to ensure the security and credibility of the business and the payment card industry.

In terms of authentication and identity management, the biggest concern within the PCI DSS is ***Requirement 8: Identify and Authenticate Access to System Components***. [xvii] This particular requirement has 8 major portions, and each of those sections has additional sub-requirements to adhere to. Implementing a proper Authentication Management solution alongside Active Directory will enable an organization to naturally adhere to these requirements with minimal effort.

Looking for More Info?
Visit the PCITechSec Blog!

Meeting the Challenges of Compliance

Active Directory anchored password management solutions support the various system access management and data protection requirements of SOX, HIPAA, GLB, and PCI. The following are compliance-related capabilities that can be achieved by Active Directory integration:

1. Facilitating and enforcing the use of stronger password policies that must be changed regularly.
2. Ensuring employees only have access to systems and information required for their specific jobs.
3. Guaranteeing accounts are disabled and access is completely revoked when employees leave company.
4. Automating password reset processes to eliminate human error
5. Ensuring complete, accurate audit trails and reports on all account changes, login attempts.
6. Confirming unified password policies via accurate password synchronization.
7. Enabling additional factors for strong and secure authentication.
8. Protecting sensitive corporate and customer data through encryption.

Active Directory
Auditing Features

An additional method of meeting the challenges of compliance is to obtain and maintain an adequate method of internal auditing. Beginning with Windows Server 2008 and on, Active Directory now supports more advanced auditing capabilities – a major factor in achieving many compliances today.[xviii] The most important feature if these updated auditing capabilities is the detail with which change logging is recorded. If an object attribute within AD is changed, both the previous and new values of said attribute can be viewed, alongside the details of who made the change and when.

These features enable various roads to achieving compliance by creating audit trails directly within the infrastructure. During a compliance audit, these logs can be viewed and analyzed as needed in order to improve the ability to track changes over the lifetime of an object (such as a User, password, etc.).

Active Directory auditing tools are not only beneficial for maintaining corporate and/or governmental compliance – appropriate use of auditing can assist with protecting an organization from potential data loss, theft, or even an attack. Tracking and monitoring adjustments made to various objects will provide an early alert to a suspicious activity on the network so that the appropriate measures can be taken to rectify the situation.

There is an entire host of benefits to Active Directory and appropriate auditing – we have only begun to scratch the surface!

"These features enable various roads to achieving compliance by creating audit trails directly within the infrastructure."

Conclusion

A vast majority of businesses throughout the world are using Active Directory in one form or another as the nexus of the company infrastructure. Proper integration and use of Active Directory opens the door to a wide array of possibilities for auditing, organization and authentication. As the saying goes, "Time is Money," and with AD, companies are better able to get back the time that is lost with password-related issues and other identity management problems.

Whether you are looking for services on-premises in your environment or in the cloud – there is an Active Directory option that will help you better serve both your organization and your end users without compromising either. It is the perfect way to increase productivity and convenience while reducing your risk.

The days of accessing a secret meeting through a single shared secret have long since passed. Gone are those moments of secrecy; traveling through the shadows, pausing at the flicker of the candlelight and letting anyone in on the secret if they know the password. The modern age demands an upgrade, and the verbal code is not enough to prove that you belong. No matter the era of history, authentication will always remain a primary concern. Active Directory offers a logical way to manage identity in the modern digital world, without compromising the security and usability that matters most.

Appendixes

Appendix 1
Adding Machines to the Active Directory Domain

Section A
Adding a Windows Machine to the Active Directory Domain

Adding a Windows 7 machine to the Active Directory Domain

- Open Windows Explorer
- Go to 'Computer' in the left-hand pane
- Click on 'System properties' at the top
- In the window that opens, click on 'Advanced system settings' in the left-hand pane
- In the new window, click on the 'Computer Name' tab at the top
- Click on the 'Change' button in the bottom-right of the window
- Enter the name of the computer as it should appear in Active Directory
- On the bottom of the same window change the radial selection from 'Workgroup' to 'Domain' and enter the name of your Active Directory Domain.
- Hit the 'Enter Key' or click on 'OK'
- Enter your Active Directory Domain administrator credentials.
- Your machine has now been added to the Active Directory Domain!

Adding a Windows 8.1 Machine to the Active Directory Domain

- In Windows Search, type in 'System' and click on the System Icon.
- Click on 'Change Settings' on the right hand side of the new window (this should be across from labels reading 'Computer Name' Domain' and/or 'Workgroup').
- In the new window, click on 'Network ID…'.
- Follow the on-screen instructions to 'Join a Domain or Workgroup'. Note: You will need Domain Administrator Credentials.

Appendixes

Adding a Windows 10 Machine to the Active Directory Domain

- Click on the Start Menu button located in the bottom left-hand corner of the screen – alternatively, simply use the 'Windows' key on your keyboard (the one that looks like the Microsoft Windows key)
- Click on 'Settings'
- Click on 'System'
- Click on 'About' in the left-hand pane.
- Click on ' Join a domain'
- Enter your Domain Name and click 'Next'
- Enter your Domain Credentials and click 'OK'.

Special Note: Using the Windows 10 Hotkey Combinations can simplify this process even further by negating the first two steps above. Additionally, you can join a domain from the 'Accounts' Menu as well. For steps, see below.

- Hold down the 'Windows Key + I' to open the settings page
- Tap or Click on Accounts
- Tap or Click on Work Access in the left-hand Pane
- Tap or Click on 'Join a Domain'

Appendixes

Section B

Adding a Mac OS X Machine to Active Directory

Binding a Mac OS X Machine to the Active Directory Domain

- Click on or open 'System Preferences'
- Click on the Padlock, located at the bottom of the right-hand pane in the new window.
  - This will allow you to make the necessary changes to Bind the machine to the domain.
  - You will be asked to enter Admin Credentials in order to make changes.
- Click on 'Login Options' just above the padlock.
- Click on the 'Join…' button in the right hand side of the window, next to 'Network Account Sever'.
- In the new Window, you will see a blank field labeled 'Server:.' Enter the fully-qualified domain name of your desired Active Directory Domain, and then click 'OK'
- The bottom of the window will alter, and ask you to provide your Domain Credentials. As noted, you must be using Admin credentials here.
  - **BE CERTAIN** to adjust the 'Client Computer ID' to a unique and properly formatted version for your chosen Domain.
- If you have done everything accordingly, the window should close, and you will be returned to the 'Login Options' screen in the 'System Preferences' window.
- If the Binding was a success, you will see a small Green Dot next to the 'Network Account Server' label.

Appendixes

Appendix 2
dsconfigad Terminal Commands

- Ex. For A System Keychain Password that does not expire enter the following command into the Terminal:

$ dsconfigad -passinterval 0

- Ex. For a System Keychain Password that expires every 30 days enter the following command into the Terminal:

$ dsconfigad -passinterval 30

Resources

[i] http://www.securitypronews.com/global-experts-speed-adoption-of-authentication-standards-2005-11

[ii] http://www.debriefdaily.com/lifestyle/password-fatigue/

[iii] https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

[iv] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731607(v=ws.10)

[v] http://www.portalguard.com/blog/2015/05/11/mac-keychain-password-recovery-the-challenges/

[vi] http://www.trackvia.com/blog/infographics/bring-your-own-devices-to-work-trend-infographic

[vii] https://wiki.jasig.org/display/CAS/CAS+Deployers

[viii] https://www.praetorian.com/blog/statistics-will-crack-your-password-mask-structure

[ix] https://www.dailymail.co.uk/sciencetech/article-2174274/No-wonder-hackers-easy-Most-26-different-online-accounts--passwords.html

[x] https://technet.microsoft.com/en-us/library/cc770394(v=ws.10).aspx

[xi] https://technet.microsoft.com/en-us/library/cc784090(v=ws.10).aspx

[xii] http://www.infosecurityeurope.com/__novadocuments/68585?v=635526151517100000

[xiii] http://www.pcworld.com/article/2685792/infographic-smb-cloud-adoption-trends-in-2014.html

[xiv] https://azure.microsoft.com/en-us/overview/what-is-azure/

[xv] https://www.sans.org/reading-room/whitepapers/compliance/compliance-primer-professionals-33538

[xvi] https://www.pcisecuritystandards.org/security_standards/index.php

[xvii] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

[xviii] https://technet.microsoft.com/en-us/library/cc731607(v=ws.10).aspx