VERIDIUM
TRUSTED DIGITAL IDENTITY

MULTI-FACTOR AUTHENTICATION WITHOUT TOKENS OR PASSWORDS

Securing Identity in Active Directory with Biometrics

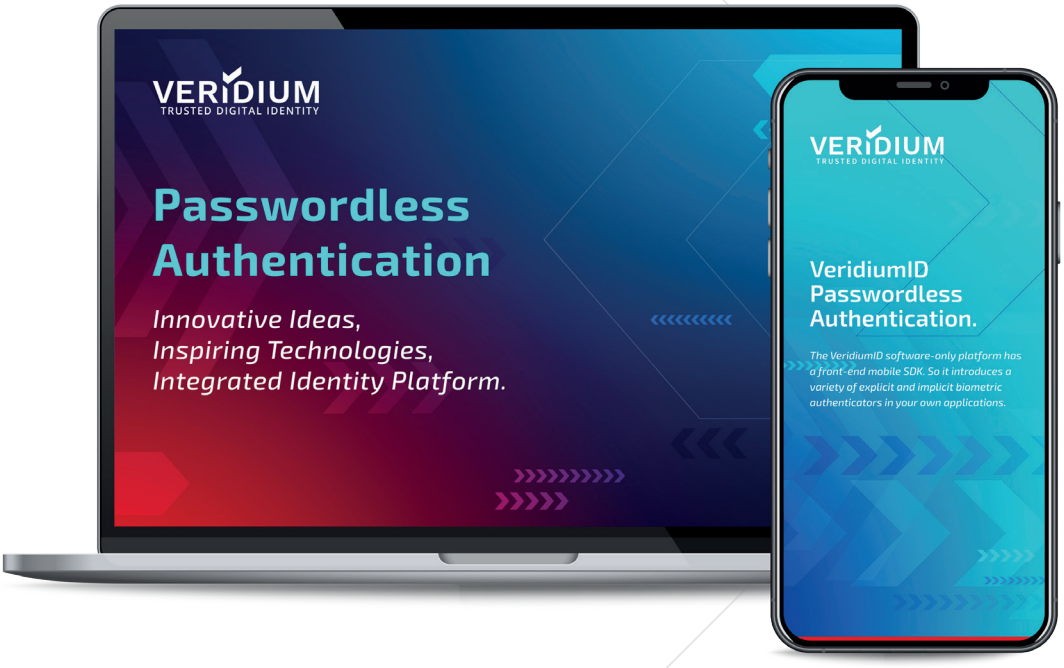
White Paper

PASSWORDS ARE AN ANCIENT PROBLEM

The idea of a password is an ancient one. Guards and sentries would ask for passwords that only those allowed entry to their camps or cities would know, ensuring the safety of the tribe. In the early years of the technology age, they seemed the natural solution for controlling access to systems that stored sensitive data. Since the 1960s passwords have been used to login into even the earliest computers, and in the 70s, the encryption of stored passwords began as a way to secure them. Since then, the complexity of both passwords and the methods used to encrypt them has evolved, but so too has the efforts of bad actors to break that encryption and steal those credentials for personal gain.

When a compromised password is used, the computer system doesn't know it. It only knows that an authorized password was entered, and grants access to whatever the associated user account is privy to. This is the fundamental flaw in the password-based security scheme. You don't know who is using the password and can never be sure whether or not their intentions are honest.

Are we going to continue using a millennia-old security solution with such an obvious flaw, or is it time to move on to other techniques the digital age has made possible and replace passwords altogether?



REPLACING PASSWORDS – THE WHY

Replacing passwords won't be an easy process. Usernames and passwords are ingrained in not only the technology we use but also the habits of the workers using that technology. The first thing we do when we boot up a computer is enter in our password, so it will take some effort to break the habit and reinforce a new one. That's why we need to deploy solutions that feel natural to use on a daily basis and help combat some of the strongest pain points organizations feel around passwords and tokens.

High Total Cost of Ownership
Both passwords and tokens have an astonishingly high total cost of ownership. Beyond simply managing these authentication tools, businesses spend time and money whenever one is lost, stolen, or forgotten. A single token can cost between $25 and $100, while password resets cost companies tens of thousands of dollars a year[1].

Lost Productivity
Beyond the costs, there's also the lost productivity that resetting passwords causes. It takes a help desk specialist upwards of 30 minutes to reset a password from receipt of the request to completion. This is lost time for the IT team as well as the employee waiting to gain access to their accounts.

The Human Element of Weak Security
Finally, there's also the very real human element that weakens security. Businesses cannot trust their employees to follow best practices when it comes to creating secure passwords and keeping them safe. The average end user will reuse the same password for 4 or more accounts, with only about 14 percent of professionals creating a unique password for every account they have[2].

REPLACING PASSWORDS – THE WHY

With the obvious reasons why businesses should replace passwords outlined, the remaining question is how. How do you eliminate a piece of security architecture so deeply ingrained within your operations, and what do you put in its place? The answer is biometrics.

The addition of biometrics is critical for achieving a strong, multi-factor authentication (MFA) solution to address the problems of access control. Biometrics provide several key improvements that no other form of authentication can provide. Namely, proof of identity.

Adding proof of identity to the mix allows enterprises to amplify security significantly, adding new verifications against their employee database and confirming additional factors for granting access permissions. For many companies, that database – the brain of their entire access management infrastructure – is Active Directory.

The integration of biometrics into Active Directory doesn't come as naturally as using usernames and passwords, but with the right tools businesses can migrate their employees to logging in with a fingerprint, face, or iris scan rapidly, providing an upgrade to both security and convenience for the end user.

1https://www.gartner.com/doc/1631318/overview-token-window-expect-pay
2http://info.gigya.com/rs/672-YBF-078/images/original-201603_gigya_infographic_deathofpassword_v11-final.jpg

BUT WHY BIOMETRICS?

Biometrics provide a unique solution for MFA, replacing something you know (a password) with something you are (your face, fingerprint, or iris). Biometrics provide a completely unique identifier you don't have to memorize, write down, or periodically reset, and they can be used to replace passwords, PINs, even hard and soft tokens.

By providing proof of identity through biometrics we gain legal non-repudiation – proof of identity by which the end user can be held legally accountable for their actions. And, with the use of modern mobile devices, we have a way to capture and securely store and transmit biometric data, all while gathering additional identifying information for numerous authentication factors to identify the end user.

Acquiring legal non-repudiation on transactions, whether it's financial or data transfer, is a large problem for organizations that are using passwords or even token-based 2FA. We're addressing this issue in a highly flexible way by delivering a software-only solution that integrates seamlessly with existing identity access management infrastructure without disrupting operations.

INTEGRATING WITH VERIDIUM'S BIOMETRIC AUTHENTICATION SOLUTIONS WITH ACTIVE DIRECTORY AND CITRIX

The first step in eliminating passwords is choosing something to replace them, which we have done with biometrics. Next, you need the platform that supports biometrics and MFA. For that, we developed VeridiumID. VeridiumID provides the rails for biometric authentication, which we can then add the different, necessary components too, such as Active Directory and/or Citrix integration.

VeridiumID installs seamlessly within your identity and access management infrastructure, without undermining existing systems. VeridiumID acts as the custom credential provider that enables biometric authentication, eliminating the need to authorize access using passwords, PINS, or tokens.

When using VeridiumAD you can have the VeridiumID server communicate with the Active Directory database, confirming the biometric match against the end user's AD profile. And, with the use of additional connectors, this sets the groundwork for single sign-on, remote access, VPN access, and more.

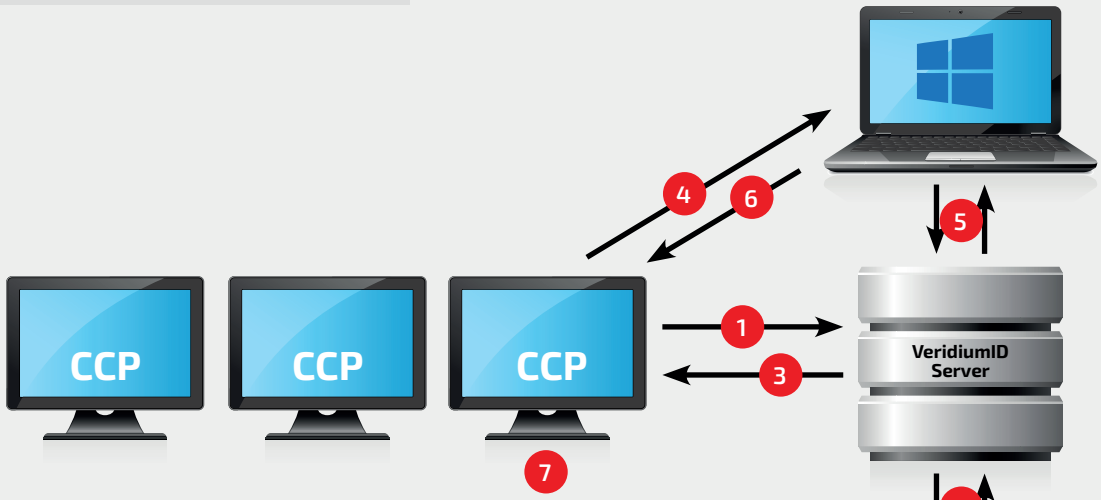
HERE ARE SOME EXAMPLES OF HOW THIS WORKS

Authenticating Employees in the Office

John heads into the office in the morning and sits down at his desk. Waking up his computer, the login screen appears. Rather than showing the line to enter a password, however, it simply displays several user icons. John clicks his name, and moments later, John gets a push notification on his phone from his company app. He opens the app and it automatically launches the biometric authentication request. John scans his chosen biometric – 4 Fingers TouchlessID, and the app works behind the scenes with the VeridiumID server software to authenticate John. Upon successful authentication, he's logged in – seconds after sitting down.

In a traditional Active Directory environment, VeridiumAD delivers a password-free use case, using biometric authentication as the primary authenticator. This method can also be configured to support offline authentication when there's no external connection to the network.

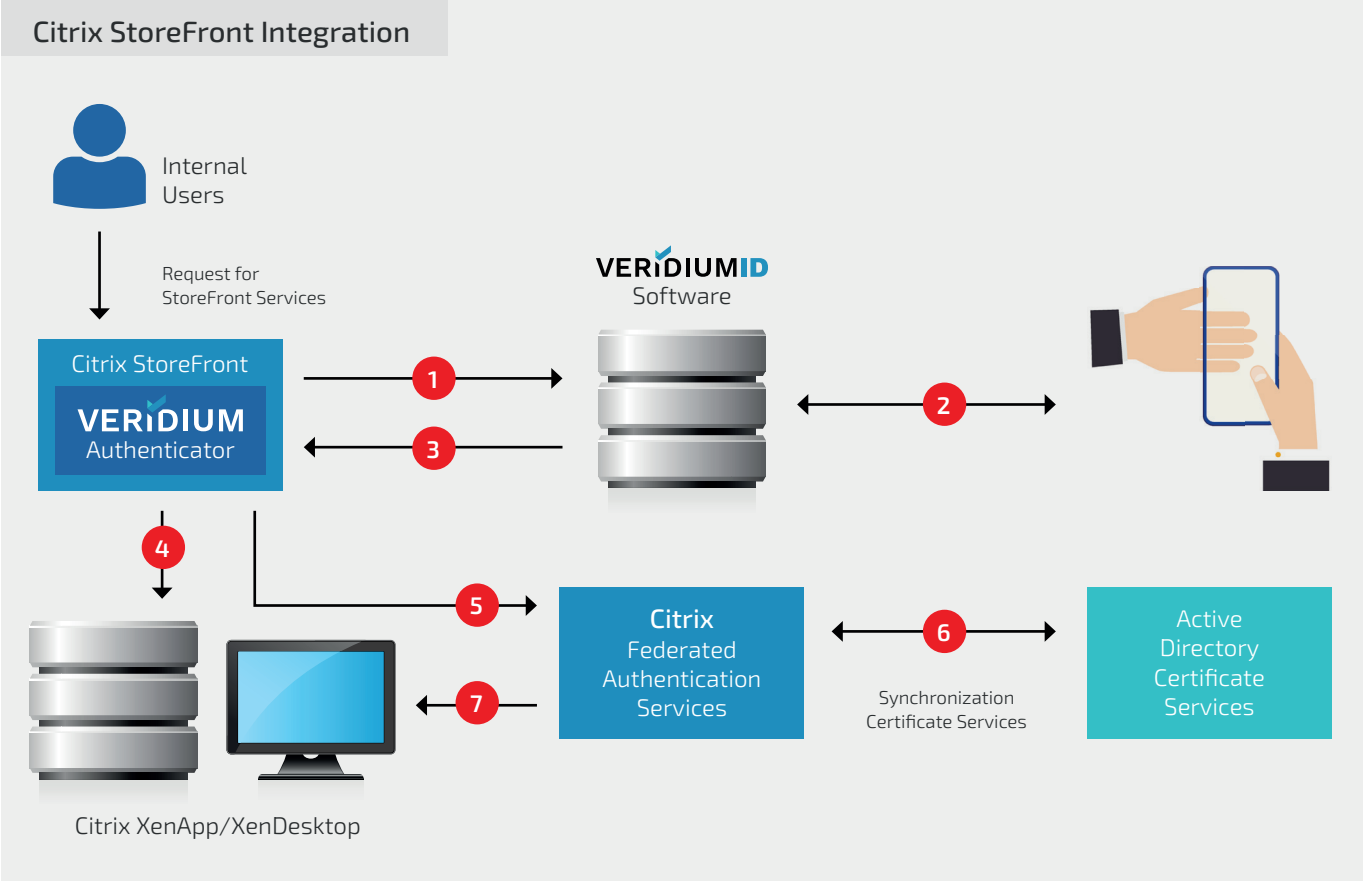
Active Directory Integration



1. Request Authentication
2. Push Notification for Biometric Authentication
3. Receive Identity Token
4. Request User Certificate
5. Validate Identity Token
6. Issue User Certification
7. Session Established

Password Replacement with Citrix StoreFront

For some enterprises, the main delivery tool for virtual environments is Citrix XenDesktop. All Citrix users on the network authenticate into Citrix StoreFront using passwords. The VeridiumAD connector for Citrix StoreFront provides biometrics as a replacement for primary authentication. The end user simply inputs their username and biometrics, and they are granted access.



1. The authenticator passes requests (along with the username) to VeridiumID.
2. VeridiumID sends a push notification to the phone for biometric authentication.
3. VeridiumID returns authentication results (success or failure) to the authenticator, which passes the result to Citrix StoreFront.
4. StoreFront displays the user's applications and desktops.
5. StoreFront contacts Federated Authentication Services (FAS) to request a certificate.
6. FAS retrieves a certificate from the Active Directory Certificate Services (PKI).
7. The application or desktop retrieves the certificate from the FAS, and the user is logged into the requested service.

CITRIX® **Ready**

"The secure delivery of apps and data, keeping people and organizations securely connected from anywhere, at all times, is our core mission for Citrix and our partners. We're pleased to name Veridium as being Citrix Ready to enhance the user experience and maintain customer and data security. Veridium provides biometric authentication of remote users in a streamlined, secure way, complementing Citrix solutions and enhancing customer mobility."

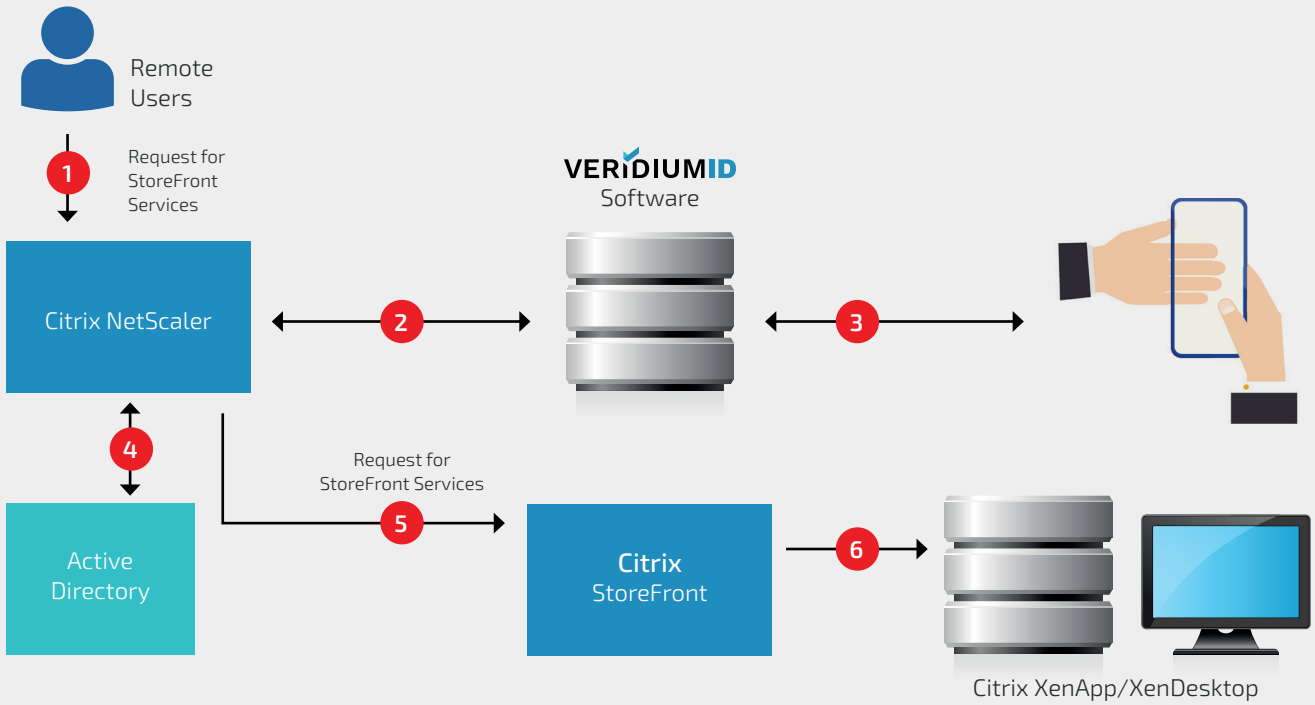
– Nabeel Youakim, Citrix VP of Products & Strategic Partners

Eliminating Tokens with Citrix NetScaler

Stephen works entirely from home for a company based in another state. When he sits down at his desk in the morning he has to log into Citrix Netscaler to access his virtual environment remotely, through a VPN. Opening the Netscaler Gateway, Stephen types in his username and password and hits Enter. Then, instead of pulling out a security token and entering that in for 2FA, Stephen receives a Push notification on his phone. Opening his company's app, he scans his 4 Fingers. His biometric is authenticated, and Stephen is logged into his Citrix environment moments later.

One of the main capabilities of Citrix NetScaler is to provide secure remote access to XenApp and XenDesktop when connecting from an external network. The VeridiumAD connector for Citrix NetScaler provides the capability to use biometrics for 2FA, rather than tokens. Replacing tokens with biometrics provides a more secure, unique identifier for authentication, establishing legal non-repudiation and reducing total cost of ownership associated with token-based 2FA systems.

NetScaler Integration



1. Remote users enter their usernames and passwords on the NetScaler sign-in page.
2. NetScaler passes the username to VeridiumID using RADIUS protocol.
3. VeridiumID looks up the mobile device for the username provided and sends a push notification for biometric authentication to the user's phone. The result (success or failure) are returned to the RADIUS client on the NetScaler gateway.
4. On success, NetScaler requests username and password authentication from Active Directory.
5. On success of both authentication factors, NetScaler accesses Citrix StoreFront.
6. StoreFront displays the user's applications and desktops.

Benefits

- Password free authentication
- Enhanced security
- Reduced total cost of ownership
- Simplified user interaction
- Verified Citrix Ready technology
- Eliminate soft and hard tokens
- Can be used as secondary or primary factor

THE ADVANTAGES OF BIOMETRIC LOGIN

Once a company has added biometrics to their Active Directory deployment, the benefits become readily apparent. Biometrics are both convenient to use and add increased security, but they also add a variety of secondary advantages depending on deployment. The Advantages of Biometric Login

Reduced Total Cost of Ownership

Password resets and replacing lost tokens is a considerable expense for any organization. Nearly half of all help desk calls in an enterprise are for resetting a password, and from start to finish this process can take at least 30 minutes. Not to mention the high cost of tokens. Whenever the company hires a new employee, or an end user loses theirs (which happens all too frequently) the firm has to purchase a new one.

Replacing passwords and tokens with mobile biometric authentication cuts these costs dramatically, providing a cheaper alternative, and one that never has to be replaced or reset.

Increased Productivity

Whenever an employee calls the help desk to reset their password it isn't just the technician losing time to this process, so is the end user. This lost productivity also contributes to the total cost of ownership, but beyond that, it's time that could be better spent at work. Furthermore, logging in with your biometrics is quick and easy, and with integrated single sign-on, employees can log in once and have swift access to all the data and services they need at their workstation, ready to go.

Legal Non-Repudiation

The primary benefit of biometrics and the proof of identity they provide is the addition of legal non-repudiation. With digital security, legal non-repudiation offers proof of the originator of any data or actions. This is verifiable proof, validated by some form of signature, in this case biometrics, that assures the sender's identity so that they cannot later deny having processed the transaction.

Biometrics automatically adds a level of trust to the digital signature for legal non-repudiation through proof of identity.

Variable Levels of Security

Due to the fact that there are numerous biometrics to choose from for authentication, businesses can easily adjust the biometrics used for various tasks based on the required level of security. Less secure biometrics like voice, face, or mobile fingerprinting can be used for low-risk tasks like checking email, while more secure ones like hand recognition or iris can be used for logging into file storage, decrypting secure communications, or authorizing financial transactions.

Secure Remote Access

Remote workers are becoming more commonplace every year, and many businesses struggle to support these highly-productive professionals. One of the biggest challenges enterprises face with a remote workforce is securing their access to internal resources. Many firms require their employees to log into a VPN to gain access to data and services, but with just a username and password there's no way to know who's on the other end of the computer. Biometric authentication significantly reduces the threat that a bad actor can gain access to an organization's VPN, providing secure login functionality and legal non-repudiation.

Conclusion

We all know that passwords pose a massive problem for enterprises around the globe, and it's time to take action. Eliminating passwords in Active Directory and Citrix environments will help stem the tide of credential-related data breaches and create a stronger foundation for further security enhancements. VeridiumAD provides the tools needed to create a password-free culture that are easy to use and deploy, without forcing your organization to change its entire IT infrastructure.

Learn more about VeridiumAD and how you can kill the password on our website: **www.VeridiumID.com/kill-the-password**

VERIDIUM
TRUSTED DIGITAL IDENTITY

London
119 Marylebone Rd
North West House
London NW1 5PU
United Kingdom
+44 1753 208780

Oxford
The Magdalen Centre
Robert Robinson Avenue
Oxford Science Park
Oxford OX4 4GA
United Kingdom

New York
1325 Avenue of the Americas
28th Floor New York 10019
United States of America
+1-857-228-7805

Romania
Bucharest
Buzesti Street 71

Press Contact
info@veridiumid.com
+1-857-228-7805

www.VeridiumID.com