Passwordless Windows Desktop Logon

CTRL + ALT + DEL without the password

What if you could remove passwords when logging onto workstations and servers and still maintain the integrity of your Windows security model?

The Windows Conundrum

If your business operates on a Windows platform, most of your users begin their workday by logging onto their Windows Desktop before navigating through multiple prompts for authentication in various on-premises and cloud-based non-AD integrated solutions. As password efficacy relies on the ability to confound hackers, these daily passwords demand complexity and frequent changes in many environments.

Despite their wide usage, passwords are a common source of frustration. Hard-to-recall cryptic combinations translate into user lockouts and forgotten passwords that cost you time and money. More worryingly, as passwords typically need to be changed regularly, users simply set weak passwords to cope with these complex controls. Worse still, passwords are always susceptible to malware and key loggers, and once compromised can be reused indefinitely. The more expansive your network, the more these pain points are likely to escalate.

What if Windows passwords could simply be removed?

Security controls and solutions have certainly matured. Administrators have access to an arsenal of tools to defend their networks from potential attack. Attacks have become more of a matter of 'when' than 'if'. When it comes to Windows, however, an Active Directory (AD) password remains a requisite for accessing most resources. Microsoft acknowledged these challenges and in order to address the issue, introduced Smart Cards as a partial passwordless solution in their Windows 2000 release. However, uptake was limited due to cost, the complexities of deploying Public Key Infrastructure, and the limitations of physical cards and readers.

Our Award-winning authentication solution is a viable alternative that satisfies your IT systems' need for secure user authentication without the exhaustive administrative burden.

Introducing the Authlogics Windows Desktop Logon Agent

A passwordless Multi-factor Authentication (MFA) solution, the Authlogics Windows Desktop Logon Agent is designed to provide your users with secure access to the Windows Desktop without the need to enter an AD password.

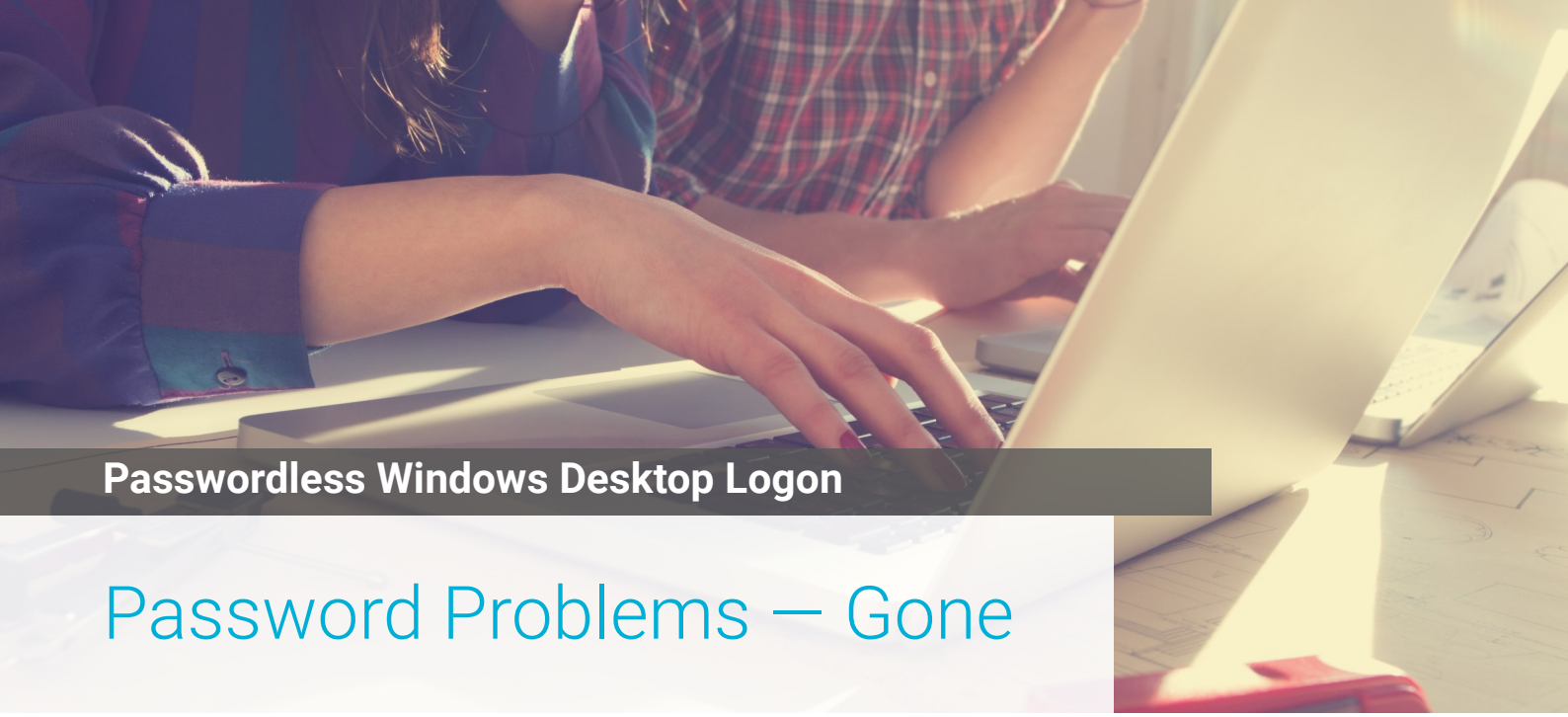
By securing the actual Windows logon process and making Windows think that a password has been entered, both local and network resources can be accessed without repeated password prompts. Applications behave exactly as if a password had been entered by the user, avoiding tedious password prompt pop-ups, password reset problems and ensuring seamless compatibility.

Simply put, you get the full Windows experience, without the passwords.

Features and highlights

- Passwordless Windows Desktop and Server logon
- Full Offline logon functionality
- Offline 2 Factor Authentication via soft token
- Tokenless 1.5 Factor Authentication
- Automatic password randomisation capability
- Group Policy based deployment
- User self-service web-based portal
- Support for Linux clients
- Patented technology

Authlogics



Passwordless Windows Desktop Logon

Password Problems — Gone

With full life-cycle Active Directory Password Security Management from Authlogics, authentication is simple, secure, and fully compliant.

How does it work?

Our Multi-Factor Authentication solution stores all your user passwords in a dedicated secure Password Vault. When logging on to a Windows desktop, users simply enter a Multi-factor One Time Code (OTC) using any of our password-less authentication technologies. Once this OTC is processed successfully, the user's password is retrieved from the Vault and provided to the Desktop Logon Agent. The agent then seamlessly injects the password into Windows, mimicking the process a user would follow if they had entered the password manually.

With this approach, Windows still receives the AD password required to function, a Windows Domain context is still created, and a Kerberos ticket is still obtained from a Domain Controller. Access to resources remains the same as always, and no functionality is lost as the underlying authentication process is preserved.

Meanwhile, the Password Vault constantly synchronises with the AD via a Domain Controller Agent, which intercepts all AD password changes on the fly.

Developed with a mobile workforce in mind

Modern businesses function best when they are flexible and responsive. Where your users need to be is not always where your network is, but you need to keep your company data secure at all times. Our Desktop Logon Agent includes an Offline Cache designed to accommodate users who need to access their desktop when they are not on the network. This cache caters for device-less 1.5 and 2-Factor logons while allowing Windows to process AD logons on the go.

For added peace of mind, offline functionality can be enabled or disabled per machine via Active Directory Group Policy.

Strong encryption

Storing passwords is a risk of its own. To mitigate this, both Online and Offline Vaults are protected by AES 256-bit asymmetric encryption using an RSA 2048 bit public/private key pair stored in a digital certificate.

During installation, a unique digital certificate is generated per workstation - ensuring no two Password Vaults are ever the same. Data can only be decrypted by authorised systems with access to the private key. Certificates can be replaced at any time and can be locked down to a specific trusted Certificate Authority (CA).

Authentication in diverse environments

With Authlogics MFA you can log onto a Web Application, Linux Server, a Wi-Fi network, or even a VPN connection without needing to use a static PIN code or a password.

If you are not ready to replace passwords just yet, then our Password Security Management solution can help you use passwords easily and securely.

Contact us today to find out how you can start transitioning your business towards a safer, more convenient password-free alternative.

Password Randomisation

Authlogics can control the full life-cycle of AD passwords to the extent that users are no longer required to enter, or even know what their passwords are. For additional protection, Authlogics Multi-Factor Authentication can automatically change specified user's passwords to a random cryptographically complex password on a regular, scheduled basis.

Because your users never need to know or enter their passwords, these can be changed daily without ever having to be concerned about accidental lockouts. You also can be assured that potentially compromised passwords are not being used on your network.

Authlogics

www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866