Password-less 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, even these daily passwords demand complexity and frequent changes to be effective.

Despite the obvious security benefits, 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 need to be changed regularly, users simply set poor 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 be removed - simply and safely?

Security controls and solutions have certainly matured. Administrators have access 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 password-less 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. Award-winning authentication experts Authlogics have now engineered 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 password-less 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 experience without passwords.

Features and highlights

- Password-less Windows Desktop and Server logon
- Full Offline logon functionality
- Automatic password randomisation capability
- Tokenless 1.5 Factor Authentication
- Offline 2 Factor Authentication via soft token
- Group Policy based deployment
- User self-service web based portal
- FIPS 198 & 180-3 compliant cryptography
- Patented technology

Authlogics

Password-less Windows Desktop Logon

Password problems? Solved!

With full life-cycle Active Directory password management from Authlogics, authentication is simple, secure, and fully compliant.

How does it work?

The Authlogics Authentication Server securely 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 Authentication Types. 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 unobtrusively 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 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 regardless of where they are initiated.

Developed with a mobile workforce in mind

Modern business functions best when it is 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 100% of the time. Our Desktop Logon Agent includes an Offline Cache Password Vault, designed to accommodate users who need to access resources remotely. This cache caters for 1.5 and 2 Factor logons while allowing Windows to process AD logons when a machine is not on the network.

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

Strong encryption

Storing passwords is a risk of its own. To mitigate this, both Server and Offline Password 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 particular trusted Certificate Authority (CA).

Authentication in diverse environments

With Authlogics Authentication Server 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.

Want to improve your security posture, while making it easier for users to access their information?

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 even more secure authentication, Authlogics can automatically change specified user's passwords to a cryptographically complex random 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 lock outs. You also can be assured that potentially compromised passwords are not being used to access your network.

Authlogics

Authlogics, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 857 214 2174