User managed passwords and MFA at the desktop

Secure CTRL + ALT + DEL with or without the password

Signing into Windows has never been so simple and secure. Meet the Windows Desktop Agent.

Passwords are problematic

With over 80% of data breaches being associated with weak, stolen or reused passwords, attacks have become more of a matter of 'when' than 'if'.

Over 1.3 billion devices run Windows with users logging in with a password. If like most business your users run Windows, most of them 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. "Complex" passwords translate into user lockouts and forgotten passwords that cost you time and money. More worryingly, as passwords traditionally need to be changed regularly, users simply set "weak" passwords to cope with these policy controls. Worse still, passwords are susceptible to phishing attacks, malware and key loggers, and once compromised can be reused indefinitely.

Removing the risk

Administrators have access to an arsenal of tools to defend their networks from potential attacks. When it comes to Windows, however, an Active Directory (AD) password remains a requisite for accessing most resources.

To alleviate the risk and costs of Windows passwords there are effectively two options: Secure them, or remove them. Either way round Authlogics has your Windows environment covered.

Passwordless logon to Windows

The Authlogics Windows Desktop Agent is a passwordless Multi-factor Authentication (MFA) solution that is designed to provide your users with secure access both online and offline to the Windows Desktop without the need to enter an AD password, and with or without a MFA device.

By securing the Windows logon process, 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.

Authlogics is also compatible with BitLocker disk encryption enabling MFA access to encrypted PCs.

Managing & Securing Windows Passwords

Not everybody is ready to go passwordless, in which case the Windows Desktop Agent provides everything you need to allow users to securely manage their passwords themselves.

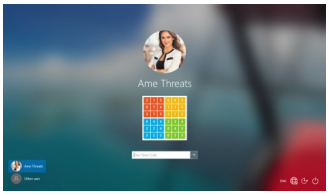
The Desktop Agent includes user-friendly password change feedback to ensure that new passwords comply with policy and are safe to use.

Forgotten your password? No problem, a simple reset with a one time code via email or SMS to get you back on track without even leaving the Windows logon screen.

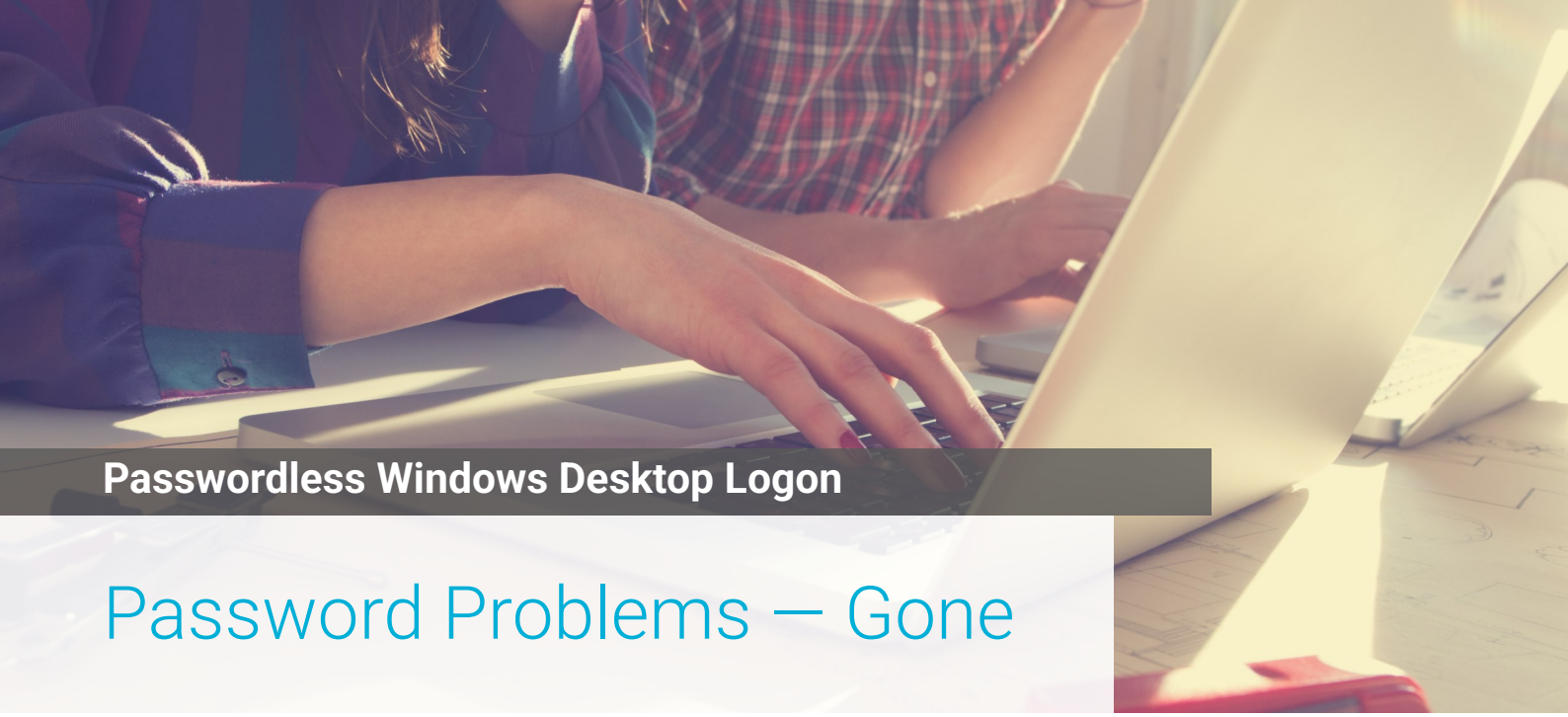
Combined with the Authlogics Authentication Server's highly granular password policy, real-time breached password protection and daily breach scanning, your users are well protected.

Features and highlights

- Passwordless MFA login to Windows Desktops
- "forgot password" reset via one time code
- Password policy compliance feedback on change
- Self-service device management
- Simple QR code registration
- Offline MFA login support
- Multiple deviceless authentication options
- Change AD passwords while out of the office
- AD Group Policy centralised management & deployment
- BitLocker disk encryption compatible



Authlogics



Passwordless Windows Desktop Logon

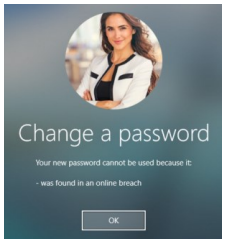
Password Problems – Gone

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

How does it work?

The Windows Desktop Agent works with the Authlogics Authentication Server to secure passwords and provide passwordless Multi-Factor Authentication (MFA). These main functions can be deployed separately or together depending on requirements.

A seemingly simple task like changing a password can become quite complicated for end users. What is the policy? How do I choose a good password? What if I forget my password?



Authlogics simplifies all this for users. Giving users exact reasons why a new password doesn't comply with the policy allows them to choose one that does. We can even send them a One Time Code (OTC) via email or SMS if they forget their password so they can reset it.

To further secure the desktop beyond passwords the Desktop Agent includes MFA. When logging on to a Windows, users simply enter an OTC using any of our authentication technologies, with or without a password.

The agent seamlessly integrates into the Windows security model, mimicking the process a user would follow if they had entered the password manually. With this approach 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.

All desktops are managed per machine via Active Directory Group Policy.

A mobile workforce

Your users are not always where your network is, but you need to keep your company data secure at all times. The Windows Desktop Agent includes offline logon functionality to accommodate users who need to access their PC when they are not on the network.

Even if the PC and phone-as-a-token are both on flight mode you can still log in. This allows users secure access to their PC with MFA no matter where they are.

Users are working from home more than ever before, however this makes changing passwords impossible without using a VPN. The Windows Desktop Agent enables users to change their Active Directory password directly in the usual way when out of the office, without a VPN.

Token Management

A common MFA challenge facing IT departments is managing users tokens.

With Authlogics, users can register their own MFA tokens via a simple QR code directly from Windows. They can also remove or enable/disable existing tokens without the need to access a web site or portal.

Authlogics allows up to 10 token devices per person providing ample coverage if one as been misplaced.

Strong encryption

All Authlogics data stored on a PC is secured protected with AES 256-bit asymmetric encryption using an RSA digital certificate.

Companies who secure data stored on PCs using BitLocker full disk encryption can now also protect access to the encrypted data with MFA.

Authlogics Password Breach Database

The Authlogics Password Breach Database is the largest enterprise compilation of over 4.1 billion credentials that have been breached, this includes over 1.25 billion unique clear text passwords making it **50% bigger than HaveIBeenPwned**. The database is hosted in the Cloud to allow for near real-time lookups and intensive data analytics.

The database powers the Authlogics Password Security Management (PSM) solution to deliver fully automated password lifecycle management. The password is safe to use when created, scanned daily to make sure it is still safe and expired if it is breached. The Desktop Agent extends this protection to end users without the usual password related headaches.

Authlogics

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