MagicEndpoint™ by WinMagic

Data Sheet

Always On Verification

USER & DEVICE VERIFICATION

MagicEndpoint provides the essential first line of defense by ensuring always-on user and device verification, eliminating user friction, and preventing costly data breaches.

After the user provides strong MFA at their OS login, the endpoint handles all authentication tasks on behalf of the user until the user logs out of their endpoint.

NO USER ACTION AUTHENTICATION | ZERO TRUST | DEVICE & USER IDENTITY

Prevent

- Session Hijacking, Phishing & AiTM Attacks
- Unauthorized Access
- Productivity Loss from MFA Fatigue

Protect

- **Endpoint Devices:** Desktops, Laptops & Servers
- **Access to Services:** Federated Web Apps (SAML, OIDC, WS-FED)
- **Legacy Systems:** RADIUS, LDAP, SSH, RDP ; Password-only apps

Authentication Security Challenges. Solved.

Traditional authentication relies heavily on point-in-time checks and easily compromised credentials. MagicEndpoint offers a revolutionary approach by combining a cryptographically secure Live Key with always-on verification. By binding the user identity to the device, MagicEndpoint ensures that access is only granted when the user is on the device and strict, continuous policies are met—all without interrupting the user.

Maximize Security with Continuous Verification

The Trusted Channel: Upon OS login, MagicEndpoint establishes a secure connection to the IdP, continuously monitoring user and device signals.

Policy Enforcement: Ensure devices meet strict conditions—encryption status, patch levels, geofencing—before, during, and after authentication.

Ultra-Short Sessions: Session tokens are shortened to 15 minutes, silently regenerated in the background to drastically reduce session hijacking risk.

99%

App/Service Coverage

SAML, OIDC, WS-FED, RADIUS, LDAP, SSH, RDP, built-in Password Manager for legacy apps

Simplify Access with "No User Action" (NUA)

Invisible Authentication: Once the Trusted Channel is established, users log into web apps and legacy systems automatically—the endpoint does all the work.

Seamless Boot to Desktop: Authenticate once at the SecureDoc boot logon and use SSO to bypass the Windows login screen entirely.

Legacy App Support: Securely access password-only applications via the MagicEndpoint Password Manager, available only when Trusted Channel policies are met.

0 %

User Actions required after Endpoint access: Users don't need to enter passwords, OTPs, tokens, etc. after strong MFA to endpoint operating system

Lower TCO with Flexible Authentication Options

Broad Token Support:
Leverage existing investments in hardware tokens like YubiKey or PIV smart cards.

Manager Approval Fallback:
Lost device? Managers can approve access remotely using their own biometrics—no helpdesk required.

15min

Session Tokens, silently renewed in the background. Supports session time customization based on your service provider's capabilities.

WINMAGIC®

US & CANADA +1 888 879 5879 | EMEA +49 69 175 370 530 | JAPAN +03 5403 6950

Technical Specifications

MagicEndpoint is built on a foundation of cryptographic rigor, broad protocol support, and flexible deployment options (SaaS, hybrid or on-prem) designed to integrate seamlessly into enterprise environments without demanding disruptive architectural changes.

The following specifications outline the authentication methods, supported protocols, and key capabilities that distinguish MagicEndpoint from legacy MFA solutions.

Authentication Methods & Protocols

Authentication Methods

- MagicEndpoint Android/iOS App – Biometrics via BLE or Out-of-Band
- Hardware Tokens (YubiKey)
- PIV Smartcards
- Passwords
- Manager Approval (Fallback)

Supported Protocols

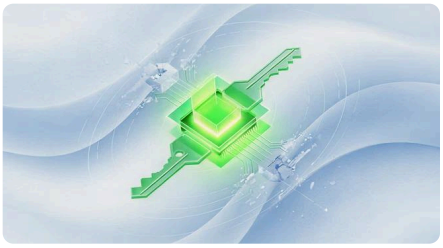
- SAML, OIDC, WS-FED
- RADIUS, LDAP, SSH, RDP

Password Manager

- Apps that don't support modern protocols
- Apps that require username/password
- ME Password Manager automatically injects specific user's password if policies are met and Trusted Channel is active

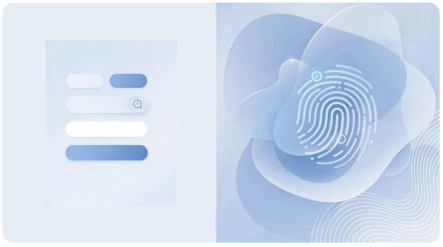
Authentication Flow

Start	
TPM-bound Live Key	Generated at OS login
Trusted Channel	Always-on verification between endpoint and IdP
Policy Enforcement	If defined policies are compliant, no user action is required
Invisible Token Renewal	Automatically renewed without user disruption
Complete	



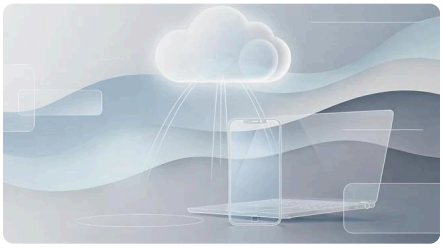
Cryptographic Device Binding

Upon successful OS login using strong MFA, MagicEndpoint combines the user identity blob with the device's TPM to generate a Live Key. This key never leaves the endpoint, establishing an unbreakable user-on-device identity that cannot be replicated or stolen by remote attackers, even in the event of a credential compromise.



Granular Step-Up MFA

Maintain a frictionless experience for routine daily tasks while enforcing elevated security for sensitive data and high-risk applications. Step-up MFA can be configured per user or per application on managed devices, requiring a biometric or hardware token prompt layered on top of the established Trusted Channel, delivering risk-proportionate enforcement without broad disruption.



Unmanaged (BYOD) Devices

Even without the MagicEndpoint client installed, users can securely access corporate web applications. The IdP recognizes the unmanaged state and prompts the user to authenticate via their configured strong method, such as the MagicEndpoint phone app, ensuring security without requiring full MDM enrollment or complex provisioning workflows.

MagicEndpoint vs. Traditional MFA

Capability	Password-Based Solutions	MagicEndpoint
Verification	Point-in-time check	Continuous – before, during, after auth
User Experience	Manual OTP, push, token codes	Zero user action after endpoint login
Session Security	Long-lived tokens	15-min session time, silently auto-renewed
Device Binding	None or cookie-based	TPM-bound Live Key, non-exportable
Phishing Resistance	Partial – OTP/push interceptable	Full – nothing to intercept
Legacy Apps	Separate vault required	Built-in Password Manager, no extra cost
BYOD Support	MDM or complex enrollment	MagicEndpoint phone app, no MDM needed
Lost Device	Helpdesk ticket	Manager approval via biometrics