

Passwordless Authentication for VPN via RADIUS

The Challenge

The rise in cyberattacks and privacy concerns has led organizations to adopt secure solutions like VPNs to protect data. With increased flexibility in remote work and BYOD policies, the need for robust digital security has grown significantly.

VPNs and RADIUS protocol

Most VPN services still rely on the RADIUS protocol, which presents two challenges:

- Complex for external IdPs or IAMs to handle.
- Some IDPs/IAMs don't support RADIUS or require extra steps to make it work.

MFA for VPN security

Companies typically use MFA to secure VPN authentication, which has pros and cons:

- Protects against unauthorized access from weak or reused passwords.
- Often ineffective against sophisticated phishing attacks.

Zero-Trust strategy

The rise of Zero Trust security has introduced challenges in implementing Zero Trust architecture:

- The [U.S. government advocates for Zero Trust](#), prohibiting SMS, OTP, push notifications, and some passwordless phone solutions.
- Many passwordless solutions suffer from the "association issue," lacking assurance that authentication requests come from legitimate endpoints.

Organizations need integrated solutions that address these vulnerabilities and align with Zero Trust principles to effectively secure remote access. By doing so, they can ensure robust protection without compromising the user experience.

Passwordless Authentication for VPN via RADIUS

The Resolution

WinMagic's MagicEndpoint is the ultimate passwordless solution, offering unparalleled security and a seamless user experience. This phishing-resistant solution can be applied to VPN access and many other remote services using RADIUS, SAML, or OIDC protocols.

Key Benefits

- **Phishing-resistant:** Protects against sophisticated phishing attacks.
- **Broad protocol support:** Works with RADIUS, SAML, and OIDC protocols.
- **Cyber insurance compliant:** Meets today's MFA requirements for cyber insurance.
- **User-friendly:** Provides the best user experience in authentication available today.

Effortless Integration

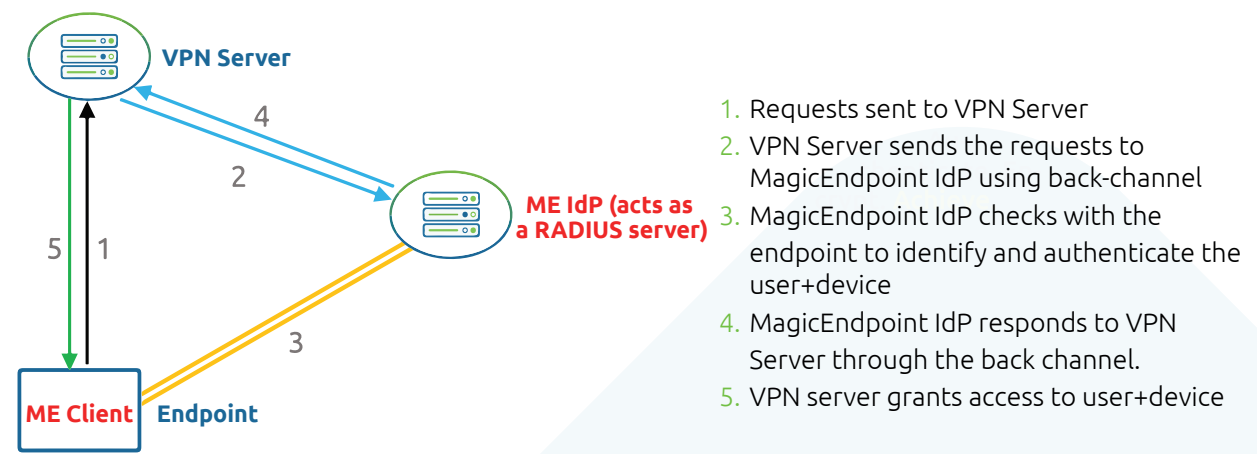
- **VPN (RADIUS) integration:** Once integrated, MagicEndpoint verifies the user's identity with MFA. Subsequent authentications occur with minimal user interaction.
- **TPM hardware protection:** Uses a securely protected key for authentication, eliminating the need for multi-factor authentication. The endpoint device handles verification without requiring external devices or additional factors.
- **User intention verification:** Ensures requests come from legitimate devices, resolving the association issue.

MagicEndpoint combines top-tier security with ease of use, making it the perfect solution for modern authentication needs. Secure your remote services with confidence and simplicity.

Simplified Deployment

- **No Additional Components Needed:** Acts as a RADIUS server for the VPN server, streamlining the implementation process.

MagicEndpoint acts similarly to a RADIUS server and doesn't require any other components, as far as the VPN server is concerned:



MagicEndpoint from WinMagic is the passwordless authentication solution that protects access by focusing on the endpoint, for the user. It requires no user action, and no third-party devices or keys, so it's seamless, secure and virtually invisible.

Authenticate. Encrypt. Achieve.