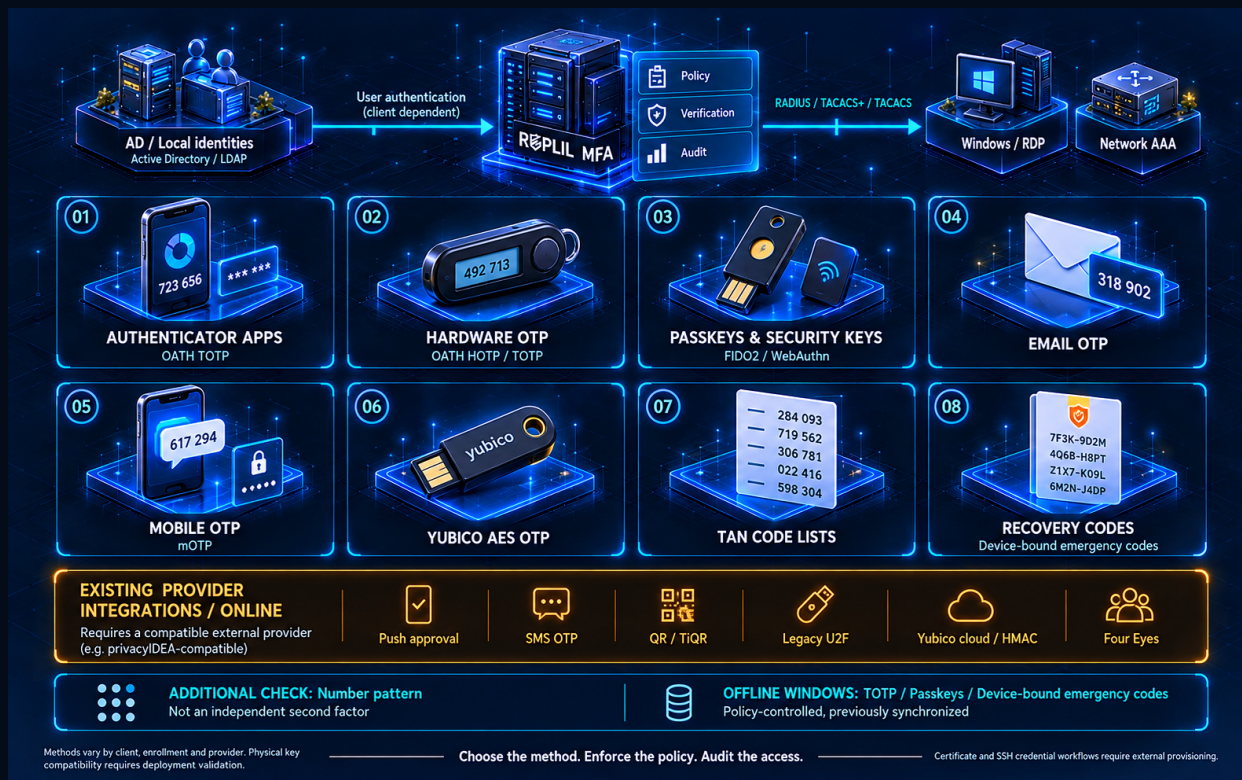


Verify identity at the access boundary.

Bring authentication, authorization and accounting into supported Windows and network-access workflows, with configured verification methods.



Illustrative workflow. Connections and permissions follow the approved deployment.

PRODUCT WORKFLOWS / KEY CAPABILITIES

01 Directory identities

Work with configured Active Directory users and groups.

02 Network AAA

Use RADIUS, TACACS+ and supported legacy TACACS workflows.

03 Verification methods

Choose supported hardware, software, OTP, pattern or email methods.

04 Accounting evidence

Review attempts, policies and network accounting activity.

The capabilities behind the workflow.

REPLIL MFA - detailed product features



AAA for network assets

Centralize authentication, authorization, and accounting with RADIUS, TACACS+, and TACACS support.



Windows and network MFA

Apply additional verification to Windows sign-in and supported network-asset access workflows.



Active Directory integration

Work with AD identities and manage authentication policies around users and groups.



Native verification methods

Authenticator apps (OATH TOTP), hardware OATH HOTP/TOTP, FIDO2/WebAuthn passkeys and security keys, email OTP, mOTP, Yubico AES OTP, TAN lists and device-bound emergency codes. Availability varies by client, enrollment and hardware validation.



Policy and provider distinctions

Number pattern is an additional knowledge check, not an independent second factor. Push, SMS, QR/TiQR, legacy U2F, Yubico cloud/HMAC and Four Eyes use compatible existing online providers. Offline Windows methods require prior synchronization and policy control.



Central administration and auditing

Review authentication activity, account policy, and network accounting from the management workspace.

Make the workflow fit the facility.



- Windows sign-in verification**
 Apply configured additional verification within supported Windows credential-provider workflows.
- Network administration AAA**
 Use supported RADIUS, TACACS+ or TACACS authentication and accounting workflows.
- Directory-aware access**
 Apply configured access policies using imported AD users and group context.

MINIMUM DEPLOYMENT RESOURCES

CPU	RAM	STORAGE
2 vCPU	16 GB minimum	100 GB SSD

Size the central service for the expected authentication rate, directory integration and retained accounting evidence. Endpoint resources and access policy depend on the supported deployment.

Windows x64 / self-contained central service

BUILT FOR CRITICAL INFRASTRUCTURE



Oil & gas



Energy & utilities



Manufacturing



Water



Smart cities



Transport

Explore your deployment with REPLIL.

replil.com / sales@replil.com