Universal MFA Server Datasheet

The MFA platform built to secure your universe. All of it.

SurePassID Universal MFA Server is the groundbreaking multi-factor authentication product that encompasses the universe of users, endpoints, applications, and operating systems that organizations must secure.

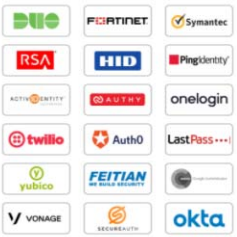
- **Any Deployment Architecture** – On-Prem, Cloud, Hybrid, Containers, Embedded, Serverless (Function-as-a-Service)
- **Any Operating System** – Windows, MacOS, Linux, Android, iOS, Embedded
- **Any Access Control App** – Windows Login, MacOS Login, RADIUS, RDP/SSH
- **Any Federated App** – SSO, ADFS, OpenID Connect, SAML, Cloud Platforms
- **Any Application** – Windows, MacOS, Linux, Android, iOS, Embedded, Hardware Appliances

As a multitenant-capable solution intended for high-security verticals such as defense, aerospace, financial, and healthcare, **SurePassID Universal MFA** ensures that multi-factor authentication can be deployed wherever it is needed or interlaced across complex network topographies and physical geographies.

SurePassID Universal MFA capabilities make it easy to deploy strong authentication for standard requirements, while a highly secure API and robust SDK can be used to secure logins to any network, application, operating system, or embedded device.

Deploy MFA everywhere and anywhere needed

Fortify your enterprise with the strongest MFA security features



Consolidate costly and inefficient legacy MFA deployments

Scale to millions of users and billions of authentications

Universal MFA Server Datasheet

The MFA platform built to secure your universe. All of it.

Specifications

Maximum Number of Users Per Server	On-Prem: 250,000 Cloud: 1,000,000 Serverless: Unlimited
Maximum Authentications Per Second	Unlimited with authentication nodes or serverless

Encryption

- AES 256 symmetric encryption
- Salted SHA 256 or 512 hashes with PKI
- TDE/TLS
- FIPS 140-2 Mode for Government/Military
- Optional Hardware Security Module (Microsoft Azure Dedicated HSM, Amazon KMS)

Deployment Options

- Windows Installer Package (Microsoft Windows Server 2008/2012/2016/2019)
- Software-as-a-Service (SaaS)
- Virtual Machine (Microsoft Hyper-V)
- Containerized (Docker/Kubernetes, Microsoft ACI, Amazon ECS)
- Serverless/Function-as-a-Service (FaaS)

Authentication Methods

- Passwordless (FIDO2)
- Username and password + OTP/PIN
- FIDO U2F, UAF, FIDO2
- OATH Event-based (HOTP)
- OATH Time-based (TOTP)
- OATH Challenge-Response (OCRA)
- Push Verification Mobile App
- Push Verification SMS OTP
- Push Verification Voice OTP
- Push Verification Email OTP
- IVR OTP
- IVR Challenge-Response
- Windows Credential Provider (WCP)
- On- and Offline Windows/MacOS Login
- Dynamic CVV for Visa/MC/Amex

Supported Authenticators

Mobile Authenticators

- Mobile OTP (smart phones, tablets)
- Browser OTP (laptops, desktops)
- FIDO virtual security keys

Hardware Authenticators

- OATH OTP keyfobs and mini-keyfobs
- OATH OTP display cards and Challenge-Response
- OATH and FIDO USB/NFC tokens (YubiKeys, etc.)
- FIDO hardware secret keys (tokens, biometric, wearable)
- OneCard Converged Credential with HID & OTP/FIDO

Temporary Passwords for Lost/Stolen/Damaged

- SMS text OTP or Push Verification (in-app)
- Email OTP, Phone OTP (Voice response)