


SurePassID Authentication Server


Secure User Access for IT/OT Systems and Critical Infrastructure

SurePassID Authentication Server is a highly extensible, highly scalable, highly available multi-factor authentication platform that secures any application, for any user and device, from anywhere, in any deployment architecture.


From the cloud to air-gapped systems, SurePassID meets the demanding authentication requirements of critical infrastructure sectors seeking to comply with cybersecurity regulations and Zero Trust mandates.

Supported Authentication Methods

 **FIDO2** – Phishing-resistant open standard that provides the highest security possible and can eliminate passwords. FIDO2 security keys can take the form of NFC, USB or BLE-enabled hardware tokens or mobile apps using secure elements.

 **OATH HOTP, TOTP, and OCRA** – One-time password (or passcode) open standard for event-based, time-based, and challenge-response authentication. OTPs can be delivered via hardware tokens (keyfobs or display cards), mobile authenticator apps, SMS, IVR, email, desktop authenticator apps, grid cards, and other means.

Push – One-tap login open standard via mobile authenticator apps on Android and iOS devices.

 **OpenID Connect** – Open standard for user authentication based on OAuth 2.0 and SAML2 that does not expose passwords. Intended for mobile and web app use cases.

Minimum Requirements

- 8GB RAM
- 200GB HD
- 2 vCPU/2 cores
- Users per server
 - Minimum: 50,000
 - Maximum: dependent on server resources

Supported Deployment Architectures

- On-Premise (including Air-Gapped)
- Private Cloud (Hosted or Data Center)
- SaaS Private
- SaaS Public
- Hybrid

Supported Deployment Options

- Windows Installer Package (.msi)
 - Microsoft Windows Server – 2008 to 2022 (any edition)
 - Microsoft Windows – 7 to 11
- Virtual Machine (Microsoft Hyper-V)
- Container Image (Docker/Kubernetes, Amazon ECS, Microsoft ACI)



SurePassID Authentication Server

Secure User Access for IT/OT Systems and Critical Infrastructure

Access Control

- Windows MFA with Offline 2FA
- MacOS MFA with Offline 2FA
- Linux MFA (PAM)
 - RHEL, SUSE, Centos, Ubuntu
- RADIUS MFA
 - TACACS+ MFA
 - FreeRADIUS MFA
- LDAP MFA
- Proxy Server MFA

Directory Integration

- Active Directory
- Azure Active Directory
- SurePassID Directory
- LDAP
- Third Party
 - Oracle, SAP, IBM, Workday, etc.

Federation

- ADFS (Active Directory Federated Services)
- SAML2 IdP
- O365 IdP
- LDAP IdP
- OIDC IdP
- Secure SSO (Single Sign-On)

Log Management

- Syslog
- Splunk
- Log4Net
- Windows Event Log
- File System
- CSV
- JSON
- JSON Flat
 - Splunk, Microsoft Sentinel, etc.

Diversity of Critical Infrastructure Sectors



Diversity of Use Cases

