# Two Factor Authentication (2FA) StoredSafe

Strong security is dependent on two factor authentication which has been a common security practice for secure conscious organizations. As the threat environment has changed, more organizations and regulators are realizing the need to further define requirements for two factor authentication to protect highly confidential information. Due to the significant risk reduction and business needs, a cost efficient solution exists to implement two factor authentication at an enterprise level for all users with access to critical and confidential information.

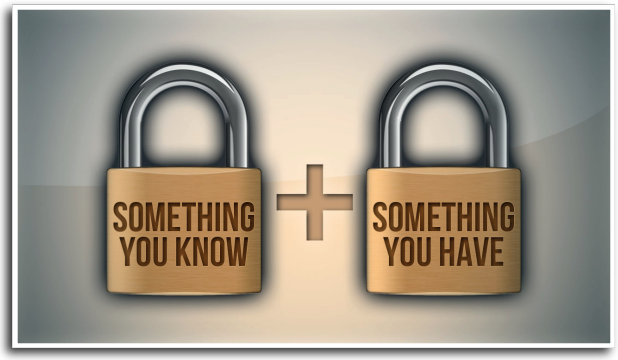
**Two Factor Authentication Made Easy!**
Two Factor Authentication StoredSafe provides organizations with a secure, easy to implement and cost-effective two-factor authentication with YubiKeys and Google Authenticator.

Our turnkey appliance enables organizations to implement two factor authentication to various information resources. It can be integrated with Active Directory other LDAPs and RADIUS, and can be integrated with any authentication and remote access solution.

**Example of Common Two Factor Authentication StoredSafe Implementations:**

- Adding 2FA to current VPN solution
- Adding 2FA for Network Equipment
- Adding 2FA to critical applications
- Adding 2FA to Unix/Linux and Windows Servers

Our solution easily integrates with your current IT infrastructure without any major redesigns.




| Defining requirements, procure and implement a two factor authentication solution could be a challenging task. Below are some of the key factors an organization should consider for a two factor authentication solution. | | | |
|---|---|---|---|
| Desired Outcome | Factors to Consider | Two Factor Authentication StoredSafe | |
| Regulatory Compliance | FFIEC, PCI–DSS, HIPAA, FISMA | Two Factor Authentication StoredSafe uses One Time Passwords (OTP) | ✓ |
| Cost Efficiency | Total Cost of Ownership (TCO) | StoredSafe has a low TCO, a low cost for implementation and annual operational cost. | ✓ |
| Scalability | Will the solution provide a full audit trail on all important events? | Two Factor Authentication StoredSafe can grow to thousands of users and implementations. | ✓ |
| Easy to implement and maintain | Implementation complexity and compatibility | Two Factor Authentication StoredSafe is compatible with all common authentication solutions. | ✓ |
| Easy to use | Usability | Two Factor Authentication StoredSafe is very easy to use. | ✓ |

StoredSafe is a premium security appliance company utilized by organizations who have strong business security requirements related to critical data that needs to be shared with internal/external parties over time and in an auditable way.

Contact | Telephone: US +1 (717) 444 1010 | Telephone: Europe +46-8-5000 2140 | E-mail:sales@storedsafe.com | https://storedsafe.com

STORED SAFE
*Secured Storage and Sharing of Highly Confidential Information*

# Technical Specifications

## StoredSafe Secure Platform

All of our products utilize the StoredSafe Secure Platform. Our unique architecture puts the information owner in control of the information on a scalable platform and enables an organization to choose between our products, based on their needs as well as adding functionality over time.

**Two Factor Authentication (2FA) StoredSafe**
**Supported Frontends**
RADIUS for 2FA and webservice for Google Authenticator and YubiKey OTP Validation.
**Supported Backends**
Windows Active Directory (AD), LDAP and RADIUS.
**Authentication Methods**
Challenge/Response, Concatenated and Secondary Authentication.
**Validation Service**
YubiKey and Google Authenticator OTP.

**Two Factor Authentication StoredSafe Overview:**
**Plug compatible to current authentication services**
Two Factor Authentication StoredSafe is designed to strengthen a current authentication service with two factor authentication.
**Two Factor Authentication Tokens**
StoredSafe can support almost any token. The current solution uses YubiKeys from Yubico. And Google Authenticator.
**HSM**
To further improve security, an HSM (Hardware Security Module) is incorporated in the platform to protect cryptographic keys for all hardware tokens. This enables our customers to be independent of Internet when in need of access to critical resources.

## Two Factor Authentication StoredSafe Implementation:

Two Factor StoredSafe is deployed between existing resources (host, router, switch, firewall, VPN etc) and the current authentication back-end to add two factor authentication. When deployed, users who authenticate to protected resources are required to add 2-factor tokens to authentication credentials.

## StoredSafe Appliance Specifications

- 1U Rack server
- Chassis with tamper detection
- Intel CPU with multiple cores and hardware random number generator support
- Redundant power supplies
- 12 TB RAIDs Storage
- YubiHSM

**Operating System and Application Standards**

- OS: Signed ISO-Image based on Ubuntu
- Database: MySQL
- CLI-GUI: Perl
- WEB-GUI: Ajax/PHP
- RESTlike: JSON
- Logging: Audit trail and syslog
- Monitoring: SNMPv3