Token-less OTP Authentication Solutions

SyferLock Technology Corporation

Next Generation Token-less Authentication Solutions

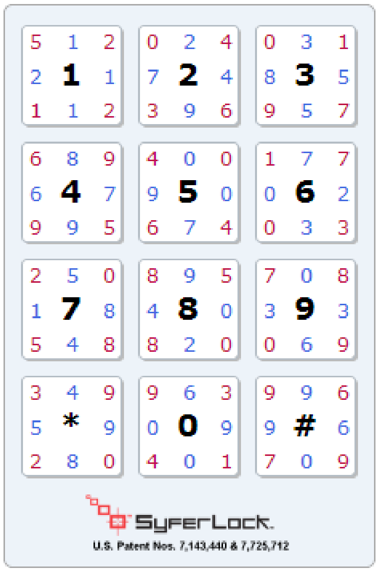
Overview

Megatrends such as the emergence of cloud computing, server and desktop virtualization, the proliferation of mobile technologies and bring-your-own-device, the increase in employees requiring remote access, and the increased use of social networking in the work environment have created new vulnerabilities and risks for companies. Users expect to access information from virtually anywhere via the Internet and mobile devices such as smart phones and tablets, and that means it is harder than ever for IT and security executives to protect an organization's information assets. One of the greatest concerns regarding security is unauthenticated access to systems and information. Given the proliferation of employees working remotely and the use of mobile devices, and the potential threat that represents for corporate networks, authentication has become a higher priority for enterprises. Username and static password alone do not provide adequate security. In addition, in some industries such as healthcare and financial services, the emergence or evolution of regulatory requirements are forcing even more stringent needs for strong authentication.

SyferLock Technology Corporation (www.syferlock.com) provides patented authentication and security solutions. SyferLock delivers two-factor and multi-factor authentication solutions utilizing patented software-based grids to convert static passwords/PINs into secure one-time passwords/PINs (OTPs). SyferLock's software-based authentication solutions provide token-less OTPs, offering a simple, more secure way to access information while leveraging existing passwords and password infrastructure. SyferLock's flexible, adaptable solutions enable enterprises to cost-effectively address two-factor and multi-factor authentication across a range of use cases and with a range of platforms. SyferLock is market validated with a growing customer list and a number of awards from independent research firms and industry publications. SyferLock was named a 2013 Emerging Technology Vendor by CRN Magazine. Increasingly, enterprises are turning to SyferLock and its superior software-based authentication solutions to strengthen security, eliminate hardware tokens and to reduce Total Cost of Ownership (TCO).

Key Features & Advantages of SyferLock's Authentication Solutions

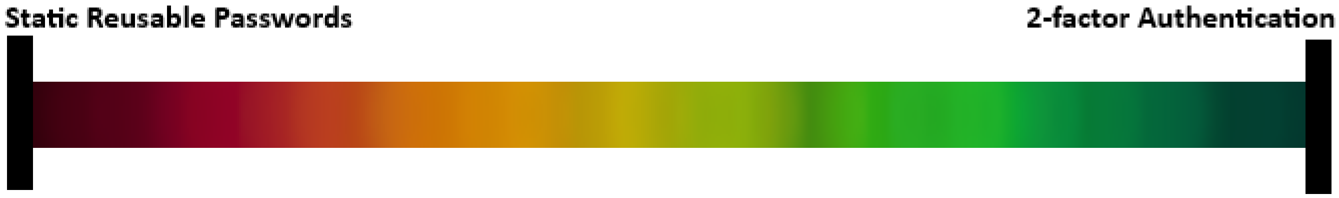
- Software-based/token-less OTP authentication
- Superior authentication and security
- Enterprise & Cloud editions
- Ease of deployment and use
- Greatly reduced TCO, both for direct and indirect costs (no tokens or token administration)



The Authentication Spectrum

Utilizing SyferLock's Solutions to Cover the Authentication Spectrum

At one end of the authentication spectrum you have commonly used static reusable passwords. At the other end of the spectrum you have 2-factor authentication. No one authentication solution seems to be flexible enough, adaptable enough and secure enough to help with ever changing business cases and user needs until now. SyferLock has created one of the most flexible, adaptable and secure authentication solutions to enable enterprises to cost-effectively address strong authentication / 2-factor authentication across a range of uses cases.



Static Reusable Passwords

At one end of the authentication spectrum you have static reusable passwords.

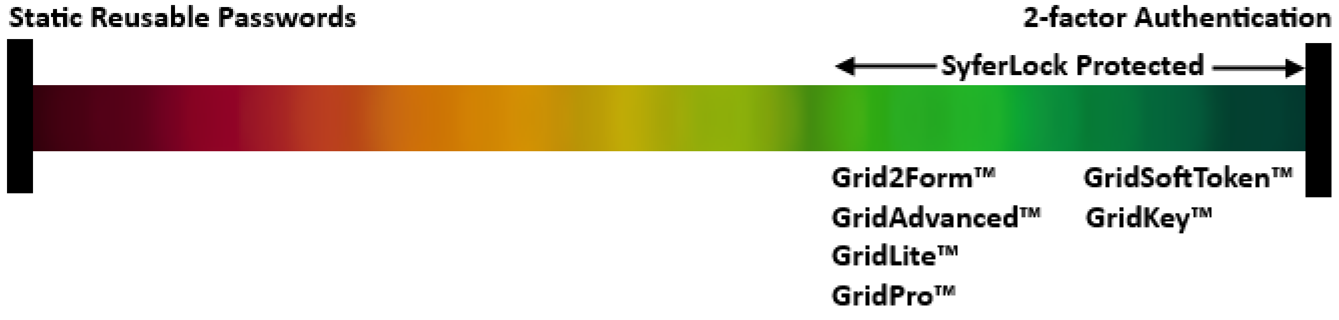
- Static passwords are weak and vulnerable to the most prevalent and easily executed attacks
- Attempts to make them "limited time passwords" that expire every 30, 60, 90 days add no real strength to the threat matrix, but add a real Total Cost of Ownership (TCO) burden to users and organizations
- Even with their known weaknesses, static passwords are the most pervasive form of authentication for the majority of organizations and users.

2-Factor and/or Multi-Factor

At the other end of the spectrum you have 2-factor, or what has historically been called strong authentication.

- While delivering increased strength, traditional hard tokens and the very nature of the "something you have" create real limitations and increased Total Cost of Ownership (TCO).
- Regulatory mandates such as PCI, SOX, FFIEC, HIPAA, CJIS and BASEL cause a heavy burden on TCO when using traditional hardware approaches to address strong authentication.
- Also, the challenge still exists to have a secure, non-intrusive "plan B" for lost, stolen, or broken devices.

Filling the Void & Covering the Authentication Spectrum



SyferLock's unique methodology covers the authentication spectrum providing two-factor and multi-factor authentication utilizing patented software-based grids to convert static passwords/PINs into secure one-time passwords/PINs (OTPs) at each log-in without the need for any additional hardware, tokens or client-side software. SyferLock addresses the weaknesses of the traditional static password without the need for any additional hardware. SyferLock eliminates or mitigates a range of attacks--

✘ Key-Logging
✘ Replay
✘ Shoulder Surfing
✘ Automated Attacks

✘ Brute Force
✘ Dictionary
✘ Sniffing
✘ Interception

✘ Stored Browser Passwords
✘ Cross Site Scripting
✘ Man-in-the-Middle

SyferLock’s Patented Approach & Methodology

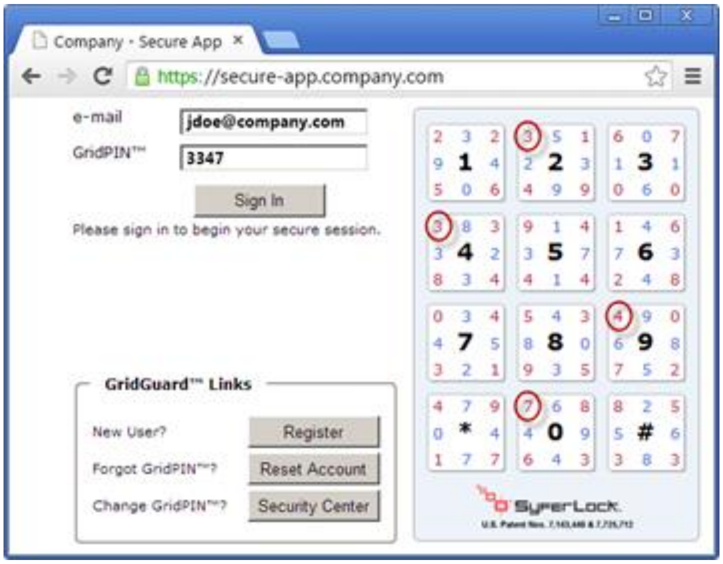
Next Generation One-Time Passwords & Enhanced Authentication

SyferLock’s patented, software-based authentication solutions provide next generation one-time passwords/PINs (OTPs) for secure access to computers, networks and the Internet. SyferLock has engineered an enhanced authentication methodology and system using token-less OTPs that provides users with a simple, more secure way to access information leveraging their existing passwords.

SyferLock delivers unparalleled flexibility through a range of solutions to address diverse and evolving authentication needs. Our zero footprint aspect provides device-less, one-time password/PIN generation without any additional client-side hardware or software. SyferLock’s methodology also allows the creation of a layered approach to current authentication processes: stand alone, or used in conjunction with other factors.

How SyferLock’s Token-less OTP Authentication Solutions Work

- At log-in, a grid (as shown below) of cells is shown, each cell containing:
  - A static number or symbol in the center, and
  - Random numbers in the corners that change with each authentication.
- User inputs the numbers corresponding to their pre-selected corner position in place of associated static password/PIN characters as their one-time password/PIN (OTP).
- For example, with a static PIN of “2490” and a pre-selected corner of “top left”, the user would input a GridPIN of “3347” for this log-in attempt.
- Upon every refresh and/or new log-in, the corner numbers randomly change, creating a new OTP.



e-mail jdoe@company.com

GridPIN™ 3347

Please sign in to begin your secure session.

2	3	2	3	5	1	6	0	7
9	1	4	2	2	3	1	3	1
5	0	6	4	9	9	0	6	0
3	8	3	9	1	4	1	4	6
3	4	2	3	5	7	7	6	3
8	3	4	4	1	4	2	4	8
0	3	4	5	4	3	4	9	0
4	7	5	8	8	0	6	9	8
3	2	1	9	3	5	7	5	2
4	7	9	7	6	8	8	2	5
0	*	4	4	0	9	5	#	6
1	7	7	6	4	3	3	8	3

These single cells with number in the corners that change with every log-in are the foundation for SyferLock’s patented software-based grids that are used to convert static passwords/PINs into secure one-time passwords/PINs (OTPs).

Product Portfolio

GridGuard™, GridPro™ & SyferLock Cloud Authentication Service™ (CAS)

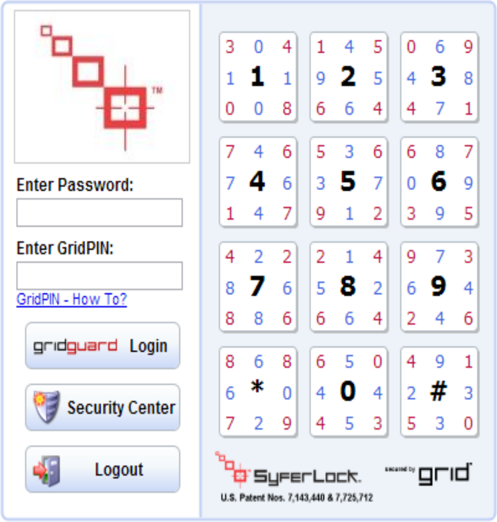
SyferLock offers enterprises a range of software-based authentication solutions, helping to identify and authenticate users before they interact with mission-critical data and applications through remote authentication (SSL VPN), intranets & extranets, web portals, e-mail, cloud computing, mobile and Microsoft Windows desktops, among other use cases. SyferLock utilizes patented software-based grids to convert static passwords/PINS into secure one-time passwords/PINs (OTPs). SyferLock's device-less OTPs offer a simple, more secure way to access information while leveraging existing passwords and password infrastructure. GridGuard™ is compliant with the accessibility requirements of Section 508 of the Rehabilitation Act.

Product	Description
GridGuard™	GridGuard™ software technology provides two-factor and multi-factor authentication for web portals, SSL VPN appliances and software applications for enterprises and governmental agencies. GridGuard's™ flexible, adaptable solutions enable enterprises to cost-effectively address multi-factor authentication across a range of use cases and with a range of platforms. GridGuard™ is deployed as a virtual appliance on the customer's network. GridGuard™ integrates with the customer's user registry to provide seamless user registration and authentication capabilities. GridGuard™ supports the following deployment models— • Grid2Form™ -- multi-factor authentication • GridAdvanced™ -- multi-factor authentication • GridLite™ -- multi-factor authentication • GridSoftToken™ -- two-factor authentication • Grid2Form™ + GridKey™ -- two-factor authentication
GridPro™	GridPro™ offers enterprises a software-based authentication solution to secure access to personal computers and tablets leveraging Microsoft's Windows® operating system platform. The GridPro™ solution consists of a log-in application (replacing the standard Windows log-in) that presents the user with a software-based grid for secure, multi-factor authentication. GridPro™ is supported on Windows laptops, desktops and servers.
SyferLock Cloud Authentication Service™ (CAS)	SyferLock's Cloud Authentication Service™ is a secure, cost-effective, cloud-based SAAS authentication service for enterprises and organizations that eliminates the complexity and burden of an in-house solution. SyferLock's Cloud Authentication Service™ provides a multi-factor, high-availability solution that uses the same patented methodology that powers SyferLock's GridGuard™ software-based authentication solutions. SyferLock's Cloud Authentication Service™ is a turn-key solution that readily integrates with most of the popular security appliances and cloud-based applications.

Flexible & Adaptable Security

Deployment Options: Grid2Form™ & GridAdvanced™ Multi-factor Authentication

Grid2Form™ - Supplementing Static Passwords with GridPINs™



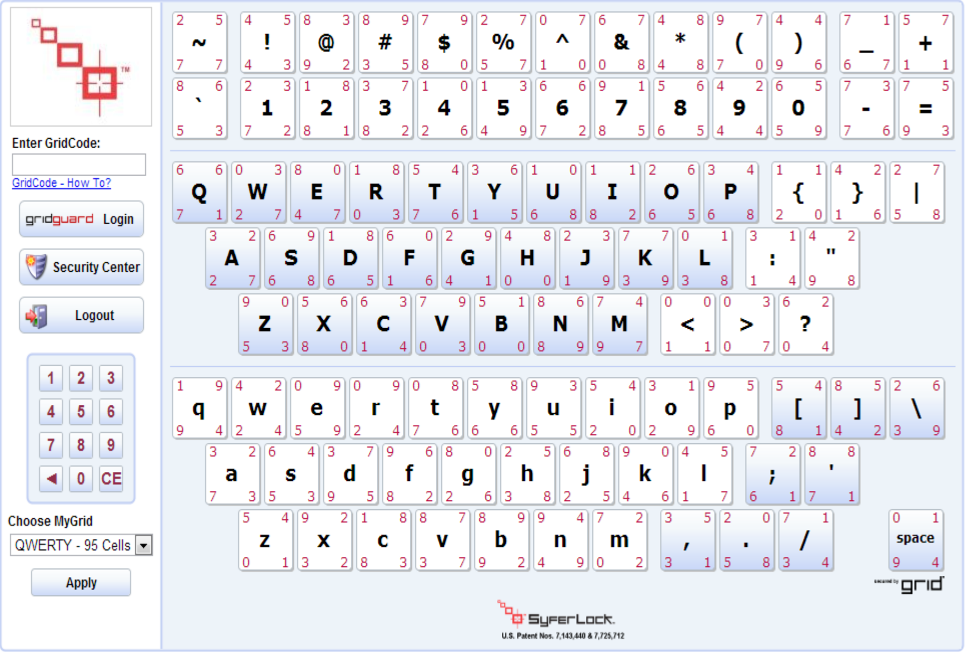
Add the power of SyferLock's patented technology by supplementing the user's enterprise user registry (typically Active Directory) password with a secure one-time PIN, the GridPIN™. This is our simplest and most popular multi-factor implementation model. Grid2Form™ is the most secure browser-based authentication solution available on the market.

Using a pre-selected PIN and target corner, the user determines their GridPIN™, and enters that in addition to the user registry password to securely log-in.

Grid2Form™ is a browser-based, zero client footprint solution that does not require any hardware tokens or smart cards and has no dependency on a cell phone like SMS-based solutions.

Grid2Form™ is available in a variety of layouts, designs, colors, languages and character sets.

GridAdvanced™ - Converting Static Passwords into GridCodes™



Choose MyGrid: QWERTY - 95 Cells

With GridAdvanced™, the user's enterprise user registry (usually Active Directory) password is strengthened by converting it into a one-time-password (OTP) using SyferLock's patented methodology. Since user passwords tend to be alpha-numeric and may contain special characters, a full QWERTY keyboard is typically used to support this implementation method.

GridAdvanced™ is a browser-based, zero client footprint solution that does not require any hardware tokens or smart cards and has no dependency on a cell phone like SMS-based solutions.

Grid Advanced™ is available in a variety of layouts, designs, colors, languages and character sets.

Flexible & Adaptable Security

Deployment Options: GridLite™ and GridKey™

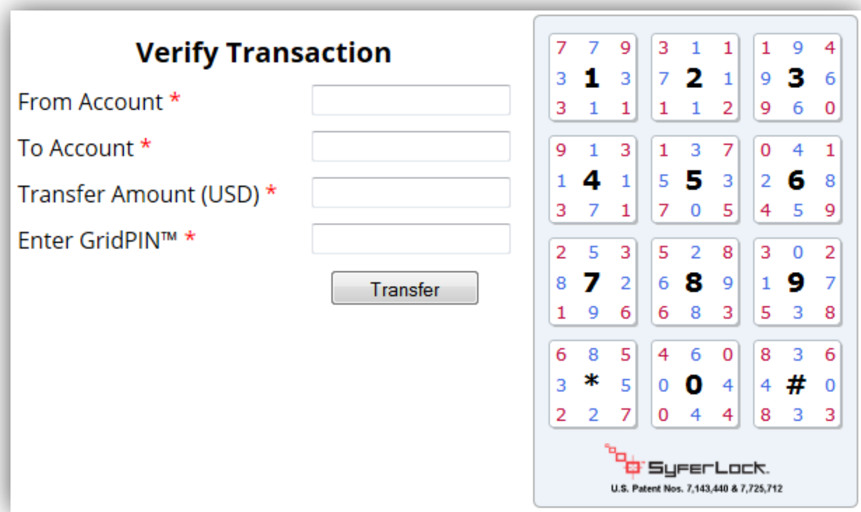
GridLite™ - Multi-factor Application & Transaction Level Security

GridLite™ is a multi-factor implementation model that allows for embedding the SyferLock authentication grid into an HTML page. The embedded component is built using Javascript and CSS, so as to be friendly to all commonly used browsers and mobile platforms. GridLite™ does not require any rich component technology like Java or Flash.

GridLite™ makes it easy to integrate SyferLock's patented technology into custom built web applications.

GridLite™ can be used to secure access to applications or for transactional level authentication; such as requiring the user to enter their GridPIN™ before performing sensitive functions within an application, such as money transfers in a banking application.

GridLite™ provides a REST based API for integration that allows the developer of the applications being integrated to very easily display the grid and validate GridPINs™.



Verify Transaction

From Account *

To Account *

Transfer Amount (USD) *

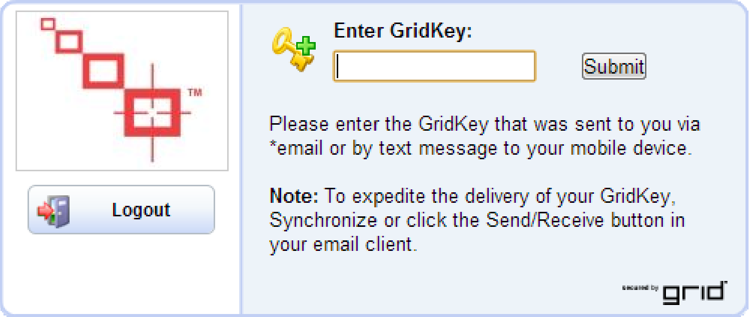
Enter GridPIN™ *

7	7	9	3	1	1	1	9	4
3	**1**	3	7	**2**	1	9	**3**	6
3	1	1	1	1	2	9	6	0
9	1	3	1	3	7	0	4	1
1	**4**	1	5	**5**	3	2	**6**	8
3	7	1	7	0	5	4	5	9
2	5	3	5	2	8	3	0	2
8	**7**	2	6	**8**	9	1	**9**	7
1	9	6	6	8	3	5	3	8
6	8	5	4	6	0	8	3	6
3	*****	5	0	**0**	4	4	**#**	0
2	2	7	0	4	4	8	3	3

Grid2Form™ + GridKey™ - 2-Factor Out-of-Band Authentication Using SMS/Email

GridKey™ is a 2-factor out-of-band authentication solution that provides the user the option to strengthen their authentication with an additional layer of security -- by sending a one-time password (OTP) to either an e-mail account or phone via SMS text message.

Unique to SyferLock is that the GridKey™ will only be generated and delivered after the user enters a valid GridPIN™ or GridCode™, creating unparalleled secure access. GridKey™ is superior to other SMS authentiication solutions.



Enter GridKey:

Please enter the GridKey that was sent to you via *email or by text message to your mobile device.

Note: To expedite the delivery of your GridKey, Synchronize or click the Send/Receive button in your email client.

GridSoftToken™

2-Factor and Multi-Factor Authentication

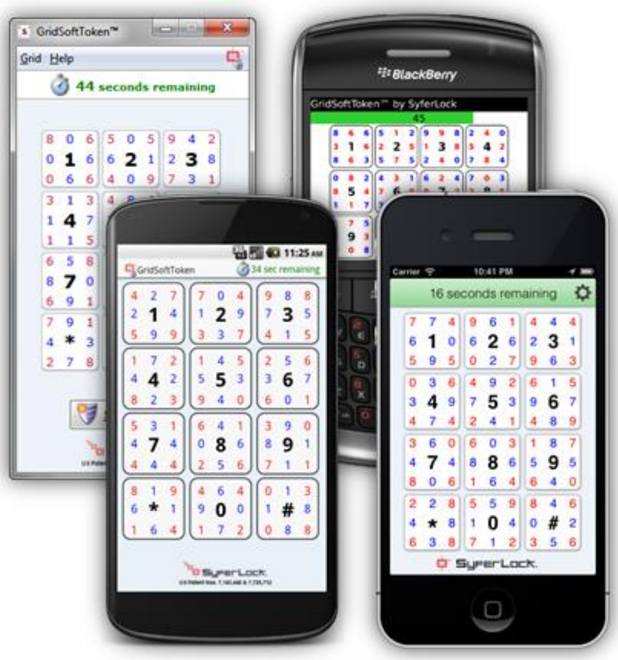
GridSoftToken™ - 2-Factor Device & User Authentication

GridSoftToken™ enables users to leverage their existing computer, laptop or smartphone as the 2nd factor for authentication. Users already "have" their device, why not leverage that instead of using a separate hard-token or smartcard?

GridSoftToken™ leverages either the underlying hardware or a user specified passphrase to generate a unique serial number specific to the device. This serial number, in combination with the device's current time, is used as the unique "seed" to generate the security grid's UI cryptograms used to log-in.

Using the displayed grid, the user determines their GridPIN™ and uses it to securely log-in.

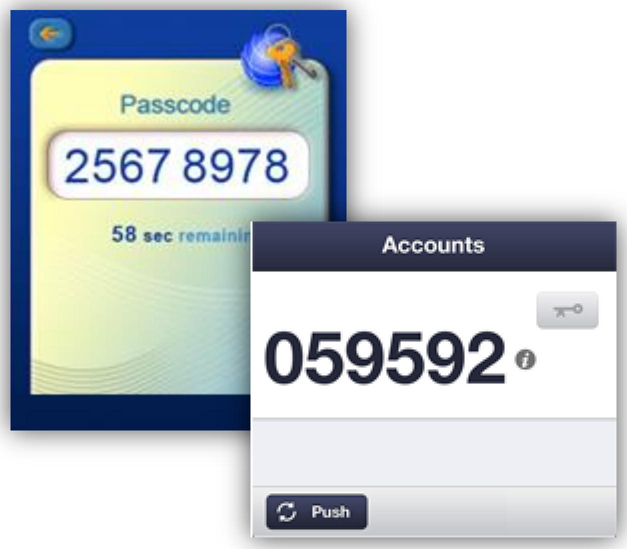
GridSoftToken™ is available as a native app on iOS, Android & BlackBerry phones and tablets. It is also available on Windows, Linux and Mac OS X desktops.



Superior User Authentication

SyferLock's proprietary technology delivers not only 2-factor device authentication, but also delivers a much higher level of user authentication. With SyferLock's GridSoftToken™, the PIN is not presented to the user "in the clear". Only the authorized user who has knowledge of the pre-selected PIN and target corner can apply the target corner to encode the PIN and generate the GridPIN™ required for log-in, making GridSoftToken™ superior to traditional soft tokens.

Images on the right show traditional soft tokens from some of the security industry's leading manufacturers. With traditional soft tokens anyone possessing access to the computer or device can read and then input the code for authentication.



GridGuard ™ Security Center

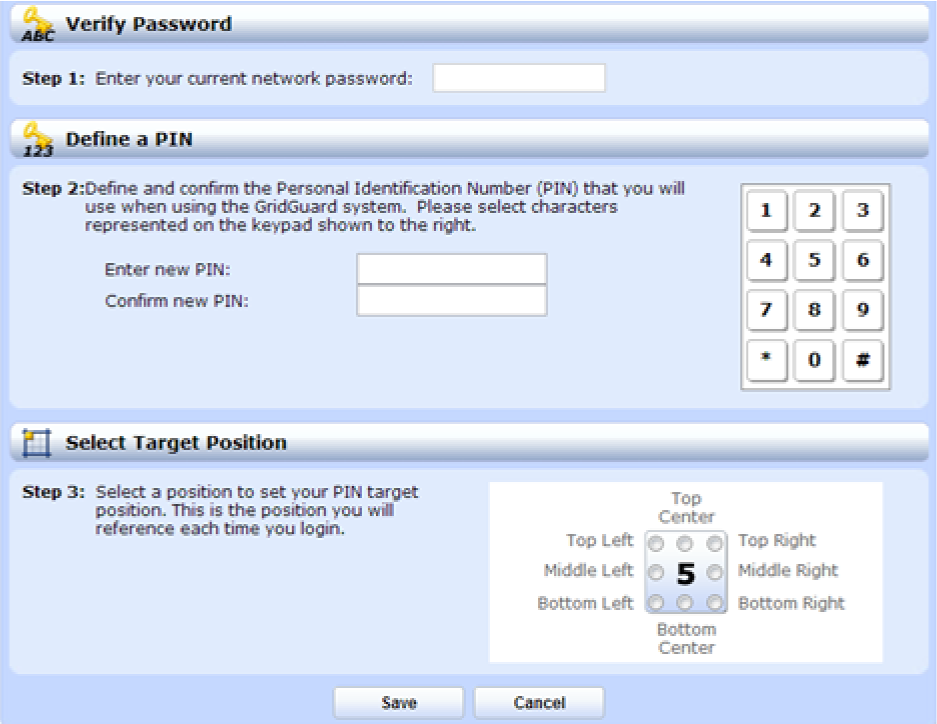
Empowering Users with Critical Self-Service Security Features

Self-Registration & Account Reset

The GridGuard™ Server allows users to register on a self-service basis relying on their enterprise user registry (typically Active Directory) password to verify their identity.

This eliminates the need for an Administrator to perform any actions to provision accounts for new users.

Users also leverage the same process to reset their accounts in the case of forgotten or expired PIN or corner/position credentials.



Verify Password

Step 1: Enter your current network password:

Define a PIN

Step 2: Define and confirm the Personal Identification Number (PIN) that you will use when using the GridGuard system. Please select characters represented on the keypad shown to the right.

Enter new PIN:

Confirm new PIN:

Select Target Position

Step 3: Select a position to set your PIN target position. This is the position you will reference each time you login.

Self-Service Management of All Grid Credentials

The GridGuard™ Server provides users access to the Security Center where users can manage their log-in credentials, without the need for intervention by an Administrator or the Help Desk. Additional self-service features include providing users with account activity logs, allowing users to manage/change their PIN/Password, corner/position, GridPic™ and other security features.

Self-Service Features	Administrator / Help Desk Functions
▪ Change Password / PIN ▪ Change Target Corner / Position ▪ Change Add-Ons & Other Security Features ▪ Change Grid Layout ▪ Change GridPic™ ▪ Account Monitoring & Anomaly Detection	▪ Deactivate Existing Users ▪ Reset User Credentials ▪ Review User Activity

GridGuard™

Security & Integration

SyferLock's GridGuard™ is an authentication server that can be installed in-house to provide best in class security. GridGuard's™ flexible, adaptable solutions enable enterprises to cost-effectively address multi-factor and two-factor authentication across a range of use cases and with a range of platforms.

GridGuard™ Security Capabilities

- SSL encrypted HTTP traffic (HTTPS)
- Protection against CSRF, XSS, SQL Injection and other attack vectors
- Data encrypted using high encryption AES-256 keys
- Separate appliance management port
- Federal Information Processing Standards (FIPS) 140-2 validation as part of the Cryptographic Algorithm Validation Program (CAVP).

GridGuard™ Integration Capabilities

- LDAP & LDAPS based Authentication
- RADIUS based Authentication
- SAML based Authentication
- REST API
    - HTTPS POST requests supporting XML / JSON formatted payloads

GridGuard™ Deployment

- Deploys as a Virtual Appliance, the GridGuard™ Virtual Appliance
- Supported on VMWare ESX/ESXi, Citrix XenServer & Microsoft Hyper-V hypervisors
- Can support all of the following deployment models:
    - Grid2Form™, GridAdvanced™, GridLite™, GridSoftToken™ and GridKey™

GridGuard™

Administration & Configuration Console (ACC)

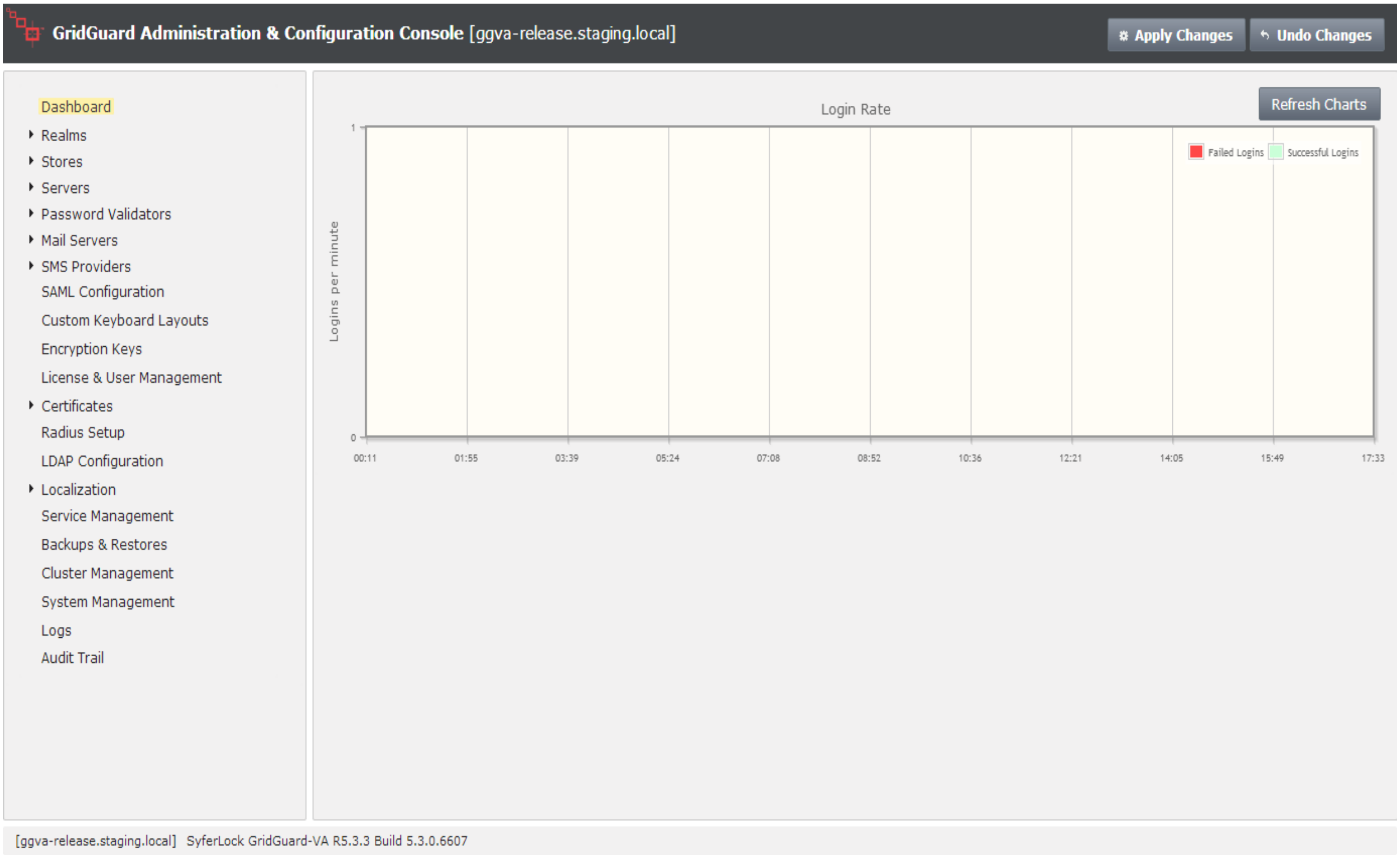
The GridGuard™ Administration & Configuration Console (ACC) provides system administrators with a web-based user interface to install, configure and manage the GridGuard™ server. Important features include:

Administration

- Ability to configure the integration with appliances / services
- Support for localization & internationalization
- Provides real time information on health and performance statistics
- Support for configuring SNMP monitoring & traps
- Support for starting and stopping services and the appliance
- SAML Configuration
- Setting log levels, viewing logs and managing log servers

Load Balancing, High Availability & Disaster Recovery

- Support for deploying multiple servers in cluster for load balancing, HA & DR
- All nodes in the cluster will replicate data to provide a fault tolerant system
- Support for online and offline, automatic and manual backups



[ggva-release.staging.local] SyferLock GridGuard-VA R5.3.3 Build 5.3.0.6607

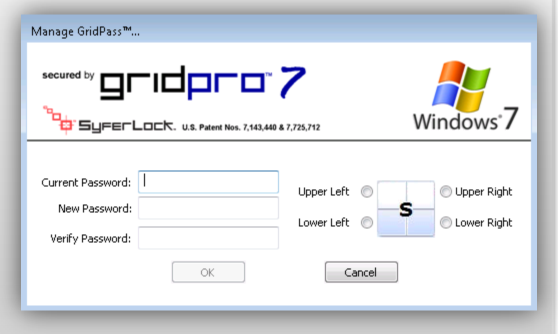
GridPro™

SyferLock’s Solution for Windows Authentication

SyferLock’s GridPro™ authentication solution is used to secure access to Windows-based laptops, desktops and servers. The GridPro™ solution consists of a log-in application (replacing the standard Windows log-in) that presents the user with a software-based grid for secure, multi-factor authentication.

The first time the user accesses the system (or any time the user changes their password), they will be prompted to select a target corner along with their password. For subsequent log-ins, the user will, using SyferLock’s one-time password methodology, input the numbers corresponding to their pre-selected corner position in place of associated static password characters as their one-time password.

Key Differentiating Factors



Current Password: |
New Password:
Verify Password:
○ Upper Left
○ Upper Right
○ Lower Left
○ Lower Right
s

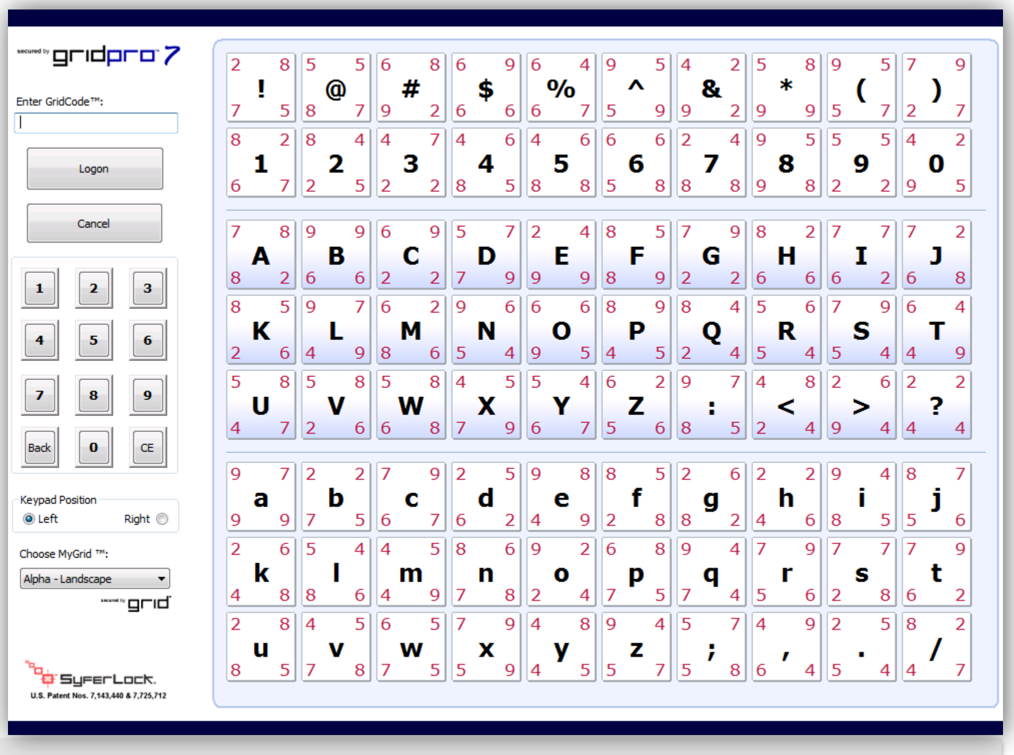
- **Strengthens Existing Password -** GridPro™ is based on user's Active Directory password; it strengthens the static password without requiring hard tokens or supplemental PINs.
- **Protection Against Attack Vectors -** By eliminating the need to enter the user's static Active Directory password, GridPro™ provides protection against attack vectors like key loggers and shoulder surfers.
- **No Connectivity Required -** GridPro™ does not require any connectivity for login. In offline mode, the user is authenticated against cached credentials.
- **Console & RDP Access -** GridPro™ protects the machine both via native console access and RDP access.
- **Multi-User Support -** With GridPro™ multiple users can log-on to the same machine with their own credentials.

Platform support for GridPro™

- Windows XP
- Windows 2000
- Windows Vista
- Windows 7
- Windows 8.1 (Fall 2014)
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

32-bit and 64-bit architectures are supported on all operating systems.

GridPro™ is delivered as an .MSI file and can be deployed either manually or using software management tools.



Enter GridCode™: |

Keypad Position ● Left Right ○

Choose MyGrid ™: Alpha - Landscape

2 8 ! 7 5	5 5 @ 8 7	6 8 # 9 2	6 9 $ 6 6	6 4 % 6 7	9 5 ^ 5 9	4 2 & 9 2	5 8 * 9 9	9 5 (5 7	7 9) 2 7
8 2 1 6 7	8 4 2 2 5	4 7 3 2 2	4 6 4 8 5	4 6 5 8 8	6 6 6 5 8	2 4 7 8 8	9 5 8 9 8	5 5 9 2 2	4 2 0 9 5
7 8 A 8 2	9 9 B 6 6	6 9 C 2 2	5 7 D 7 9	2 4 E 9 9	8 5 F 8 9	7 9 G 2 2	8 2 H 6 6	7 7 I 6 2	7 2 J 6 8
8 5 K 2 6	9 7 L 4 9	6 2 M 8 6	9 6 N 5 4	6 6 O 9 5	8 9 P 4 5	8 4 Q 2 4	5 6 R 5 4	7 9 S 5 4	6 4 T 4 9
5 8 U 4 7	5 8 V 2 6	5 8 W 6 8	4 5 X 7 9	5 4 Y 6 7	6 2 Z 5 6	9 7 : 8 5	4 8 < 2 4	2 6 > 9 4	2 2 ? 4 4
9 7 a 9 9	2 2 b 7 5	7 9 c 6 7	2 5 d 6 2	9 8 e 4 9	8 5 f 2 8	2 6 g 8 2	2 2 h 4 6	9 4 i 8 5	8 7 j 5 6
2 6 k 4 8	5 4 l 8 6	4 5 m 4 9	8 6 n 7 8	9 2 o 2 4	6 8 p 7 5	9 4 q 7 4	7 9 r 5 6	7 7 s 2 8	7 9 t 6 2
2 8 u 8 5	4 5 v 7 8	6 5 w 7 5	7 9 x 5 9	4 8 y 4 5	9 4 z 5 7	5 7 ; 5 8	4 9 , 6 4	2 5 . 5 4	8 2 / 4 7

SyferLock Cloud Authentication Service™

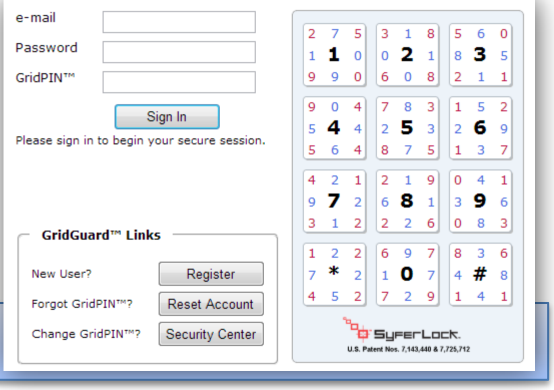
SyferLock's SAAS Authentication Solution

Authentication as a Service

SyferLock's Cloud Authentication Service™ is a secure, cost-effective, cloud-based authentication service for enterprises and organizations that eliminates the complexity and burden of an in-house solution.

Strong authentication has become a challenge for many enterprises and organizations, with employees, contractors, partners and customers requiring access to an organization's systems, applications and data. Deploying and supporting in-house authentication solutions to address this challenge can require a significant initial and on-going investment in financial resources and personnel. With no additional infrastructure required, enterprises can rapidly deploy SyferLock's Cloud Authentication Service™ to cost-effectively address strong authentication.

SyferLock's Cloud Authentication Service™ provides a multi-factor, high-availability solution that uses the same patented methodology that powers SyferLock's GridGuard™ two-factor and multi-factor authentication solutions.

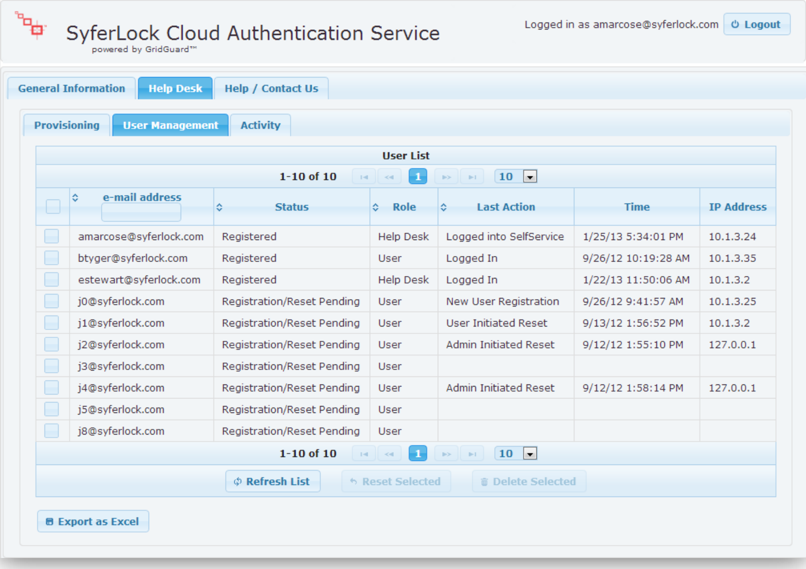


Please sign in to begin your secure session.

2	7	5	3	1	8	5	6	0
1	**1**	0	0	**2**	1	8	**3**	5
9	9	0	6	0	8	2	1	1
9	0	4	7	8	3	1	5	2
5	**4**	4	2	**5**	3	2	**6**	9
5	6	4	8	7	5	1	3	7
4	2	1	2	1	9	0	4	1
9	**7**	2	6	**8**	1	3	**9**	6
3	1	2	2	2	6	0	8	3
1	2	2	6	9	7	8	3	6
7	*****	2	1	**0**	7	4	**#**	8
4	5	2	7	2	9	1	4	1

Key Differentiating Factors

- **Turn-key Integration -** Turn-key solution that readily integrates with most of the popular security appliances and cloud-based applications.
- **Lower Costs –** Eliminates the need for in-house IT infrastructure and thereby reduces the cost for hardware, software and personnel to manage the solution.
- **Managed System Uptime, Upgrades & Updates -** SyferLock manages availability of the system, as well as all system upgrades/updates; there is no need for customers to add hardware, software or bandwidth as their user base grows.
- **Scalable -** SyferLock's multi-tenant architecture allows the service to scale to meet customer demand.



Logged in as amarcose@syferlock.com

User List

1-10 of 10 | 1 | 10

	e-mail address	Status	Role	Last Action	Time	IP Address
□	amarcose@syferlock.com	Registered	Help Desk	Logged into SelfService	1/25/13 5:34:01 PM	10.1.3.24
□	btyger@syferlock.com	Registered	User	Logged In	9/26/12 10:19:28 AM	10.1.3.35
□	estewart@syferlock.com	Registered	Help Desk	Logged In	1/22/13 11:50:06 AM	10.1.3.2
□	j0@syferlock.com	Registration/Reset Pending	User	New User Registration	9/26/12 9:41:57 AM	10.1.3.25
□	j1@syferlock.com	Registration/Reset Pending	User	User Initiated Reset	9/13/12 1:56:52 PM	10.1.3.2
□	j2@syferlock.com	Registration/Reset Pending	User	Admin Initiated Reset	9/12/12 1:55:10 PM	127.0.0.1
□	j3@syferlock.com	Registration/Reset Pending	User			
□	j4@syferlock.com	Registration/Reset Pending	User	Admin Initiated Reset	9/12/12 1:58:14 PM	127.0.0.1
□	j5@syferlock.com	Registration/Reset Pending	User			
□	j8@syferlock.com	Registration/Reset Pending	User			

1-10 of 10 | 1 | 10

SyferLock's Cloud Authentication Service™ is also available for resellers and third-party service providers for their end-user customers. Resellers and service providers can manage their customers from a multi-tenant platform enabling an easy migration to a centralized cloud environment with minimal disruption to end users.

Integrated Platforms

Supported Applications, Appliances & Platforms

With its open standards-based architecture, SyferLock's GridGuard™ is interoperable with applications, appliances and platforms that offer support for external authentication mechanisms including LDAP, RADIUS and SAML. These platforms include everything from hardware appliances like Cisco Netscalers and Juniper SA devices to pure software applications like Salesforce & Google Apps. Below are some of the platforms that have been integrated with GridGuard™. All of these implementations are supported on both Enterprise & Cloud Editions of GridGuard™.

Product	Version	Grid2Form™	GridAdvanced ™	GridLite™	GridSoftToken™	SAML
Array Networks AG	All	Yes	Yes	Yes	Yes	--
Array Networks SPX	All	Yes	Yes	Yes	Yes	--
CA Siteminder	All	Yes	Yes	Yes	Yes	Yes
CheckPoint Connectra	6.5+	Yes	Yes	Yes	Yes	--
Cisco ASA (Clientless)	All	Yes	Yes	Yes	Yes	--
Cisco ASA (IPSec)	All	--	--	--	Yes	--
Cisco IOS Management Console	All	--	--	--	Yes	--
Citrix Access Gateway	4.5 Adv	Yes	Yes	Yes	Yes	--
Citrix Access Gateway	4.6 Std+	Yes	Yes	Yes	Yes	--
Citrix Netscaler / Access Gateway Ent. Ed.	8.2+	Yes	Yes	Yes	Yes	--
Dell vWorkspace	All	--	--	--	Yes	--
F5 BIG IP	All	--	--	Yes	Yes	--
ForgeRock OpenAM	All	Yes	Yes	Yes	Yes	Yes
Google Apps	All	Yes	Yes	--	--	Yes
IBM Tivoli Access Manager (TAM-ESSO)	All	--	--	Yes	Yes	--
Joomla	1.5+	Yes	Yes	Yes	Yes	Yes
Juniper SA	6.2+, 7.x	Yes	Yes	Yes	Yes	Yes
Microsoft Forefront UAG	2010	--	--	Yes	Yes	--
Microsoft Office 365	Current	Yes	Yes	--	Yes	--
Microsoft Outlook Web Access	2003 – 2010	--	Yes	--	--	--
Okta	All	Yes	Yes	Yes	Yes	Yes
PingFederate / PingOne	All	Yes	Yes	Yes	Yes	Yes
Salesforce	All	Yes	Yes	--	--	Yes
Sonicwall Aventail EX Series	10.0	Yes	Yes	Yes	Yes	--
Sonicwall SSL-VPN 2000	All	--	--	--	Yes	--

Token-less OTP Authentication Solutions

SyferLock Technology Corporation

917 Bridgeport Avenue
Shelton, CT 06484
USA

Phone +1-203-292-5441
Fax +1-203-941-0575

info@syferlock.com
www.syferlock.com