SyferLock's Cloud Authentication Service

powered by GridGuard™

An Introduction

The Problem

- Need Strong Authentication
  - Protect access to applications / appliances
  - Username + Password alone considered vulnerable

- Need Universal Access
  - Ability to authenticate from a variety of client devices
    - Laptops, desktops, mobile devices incl. phones & tablets
  - Ability to authenticate from anywhere
    - Work, Home, On the road
  - Ability to leverage the same authentication solution across platforms
    - Remote VPN, SAAS / Web Portals, etc.

- Keep TCO Low
  - Keep capital investment, support & upgrade costs low

The Solution

- **SyferLock's Cloud Authentication Service**
  - Patented Grid based authentication technology
    - Secure method of authentication
    - Software based; device-less one-time PIN (OTP) authentication
  - Hosted in the SyferLock Cloud
    - No server deployment required on-site
    - No access to customer user registry (LDAP/AD) required
    - Subscription based licensing (pay-as-you-use)
    - Lower initial costs
    - Painless upgrades
  - Accessible from any device with a web browser
  - Integrates with a range of applications / appliances
  - User friendly

SyferLock Methodology Explained

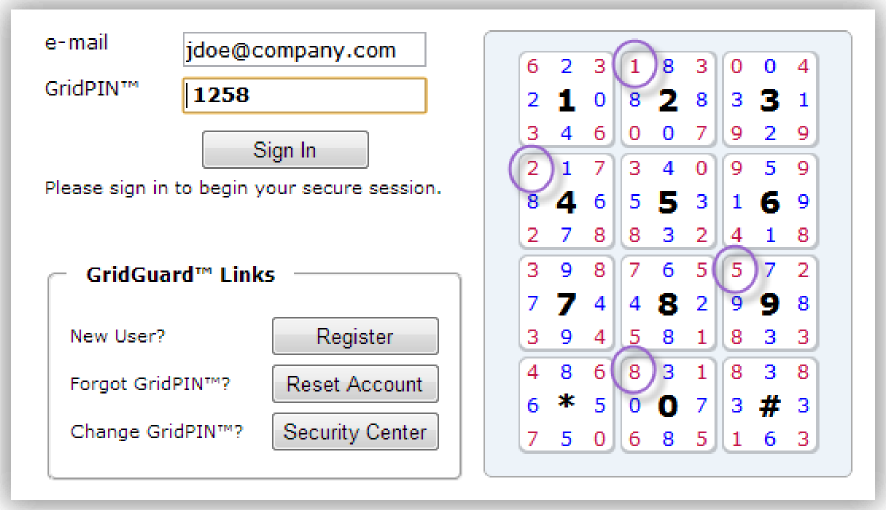
- Static PIN is "formularized" to generate a secure one-time PIN (aka GridPIN™)

- A grid of cells is displayed, each cell containing
  - A static number or symbol in the center, and
  - Random numbers in each cell corner, which change with each authentication

- User inputs numbers corresponding to their pre-selected corner position in place of associated static PIN characters

- A GridPIN™ can map to multiple PIN & corner combinations

- An example
  - If the static PIN is '2490', and
  - the pre-selected corner is 'top left'
  - ➢ GridPIN™ is '1258', for this attempt



e-mail: jdoe@company.com

GridPIN™: 1258

Please sign in to begin your secure session.

GridGuard™ Links

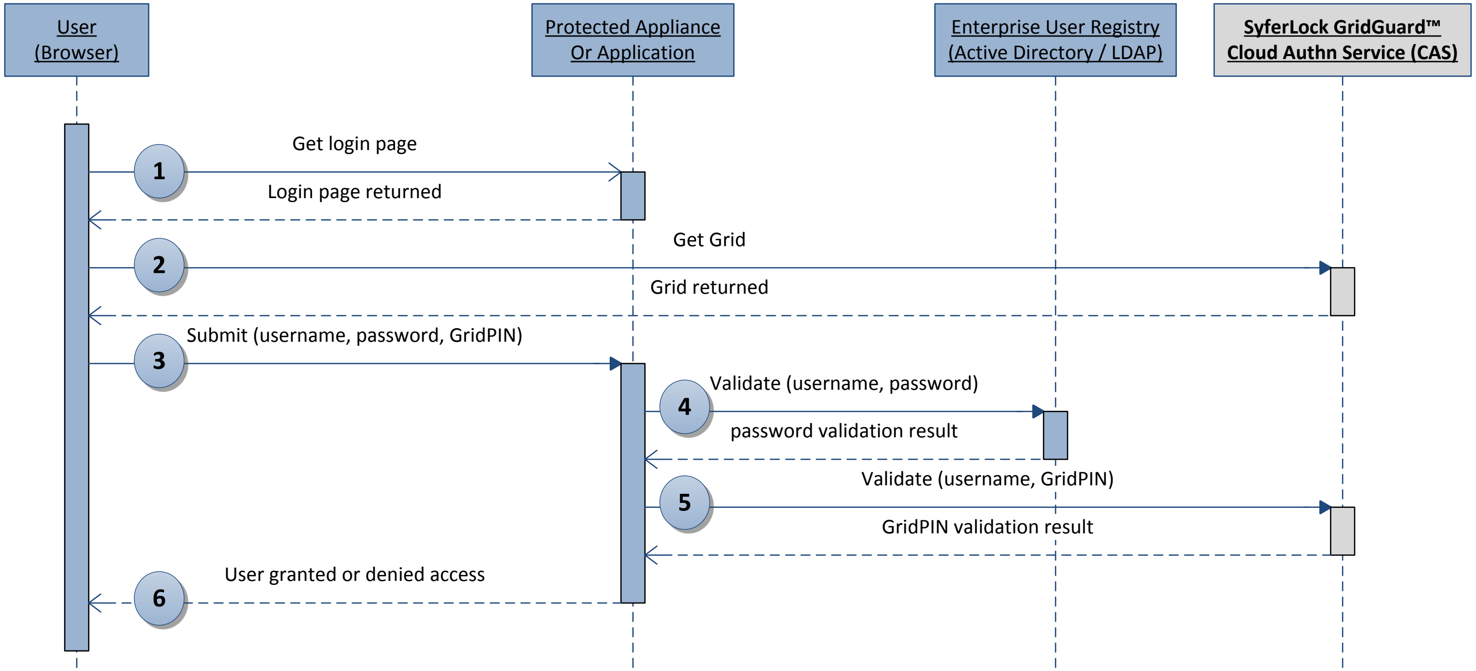
New User?

Forgot GridPIN™?

Change GridPIN™?

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

Authentication Explained


User (Browser)
Protected Appliance Or Application
Enterprise User Registry (Active Directory / LDAP)
SyferLock GridGuard™ Cloud Authn Service (CAS)
1
Get login page
Login page returned
2
Get Grid
Grid returned
3
Submit (username, password, GridPIN)
4
Validate (username, password)
password validation result
5
Validate (username, GridPIN)
GridPIN validation result
6
User granted or denied access

1. User accesses authentication page on protected appliance or portal
2. Authentication page requests a grid from the CAS server
   An instance of a grid is returned and embedded in the page
3. Security appliance validates the password against the enterprise user registry
4. Appliance validates the GridPIN™ against CAS (via LDAPS or REST API Interface)
5. If both enterprise user registry and CAS respond back in the affirmative, user is authenticated and granted access

GridPIN™ Validation

- Secured Appliance / Web portal can validate GridPIN™ in 2 ways:
  - LDAP
    - Protocol supported over SSL (LDAPS)
  - REST API
    - SSL encrypted HTTP POST requests (HTTPS)

User Registration

- Two Enrollment Modes Supported

Criteria	Open Enrollment	Limited Enrollment
Who is allowed to register	Any user with a valid email address registered to the domain can register	Administrator defines the users within the domain who are allowed to register
How users Register	Registration is self-initiated by user	Registration is initiated by Administrator
Licensing	All users within the domain will be allowed to register subject to license limits; may need to purchase as many licenses as users	Only the named users within the domain will be allowed to register. Number of licenses purchased can be limited to number of named users

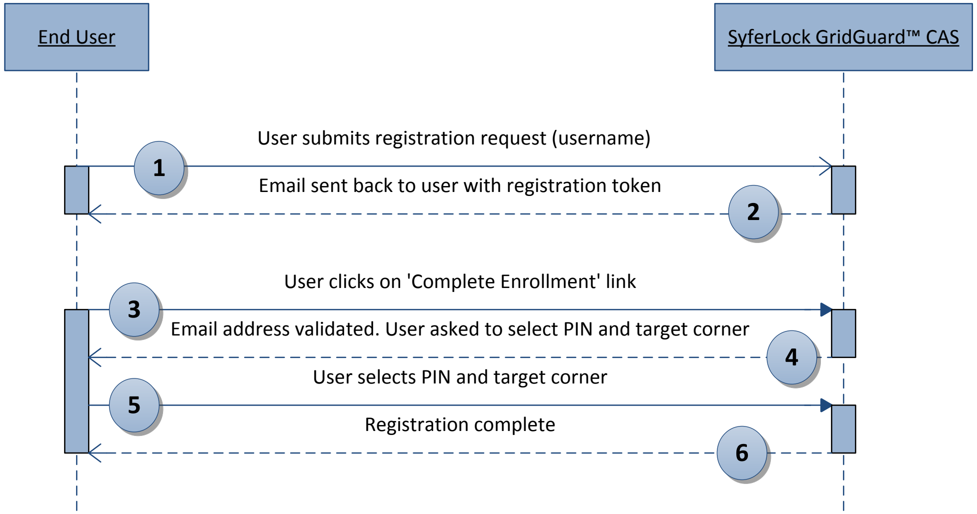
Summary

- SyferLock's Cloud Authentication Service provides:
  - Strong Authentication as a Service
  - Patented GridGuard™ Multi-factor Authentication Methodology
    - Software based; device-less one-time PIN (OTP) authentication
  - Low Total Cost of Ownership (TCO)
    - No hardware or virtual appliance to install
    - No support costs
    - No upgrade costs
    - No capital investment
    - Pay-as-you-use service (no long term commitment)
    - 24 x 7 support from SyferLock

Appendix

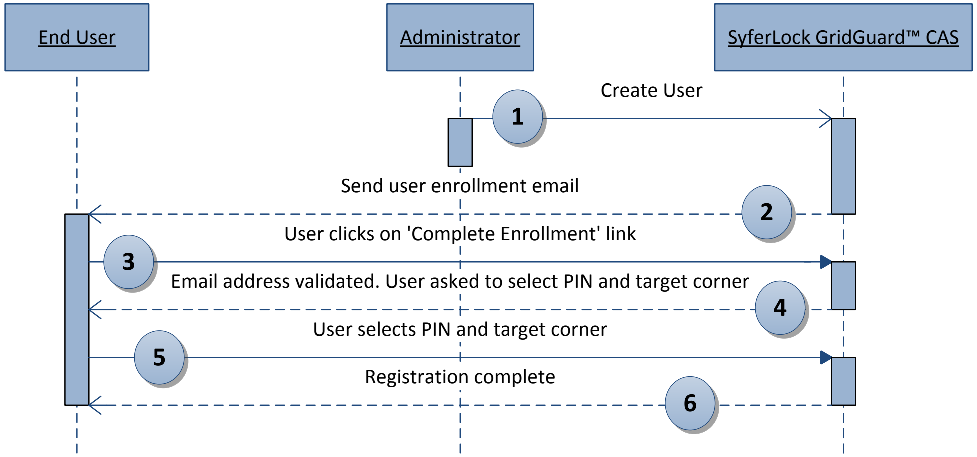
TECHNICAL SPECIFICATIONS

Registration - Open Enrollment


End User
SyferLock GridGuard™ CAS
1
User submits registration request (username)
2
Email sent back to user with registration token
3
User clicks on 'Complete Enrollment' link
4
Email address validated. User asked to select PIN and target corner
5
User selects PIN and target corner
6
Registration complete

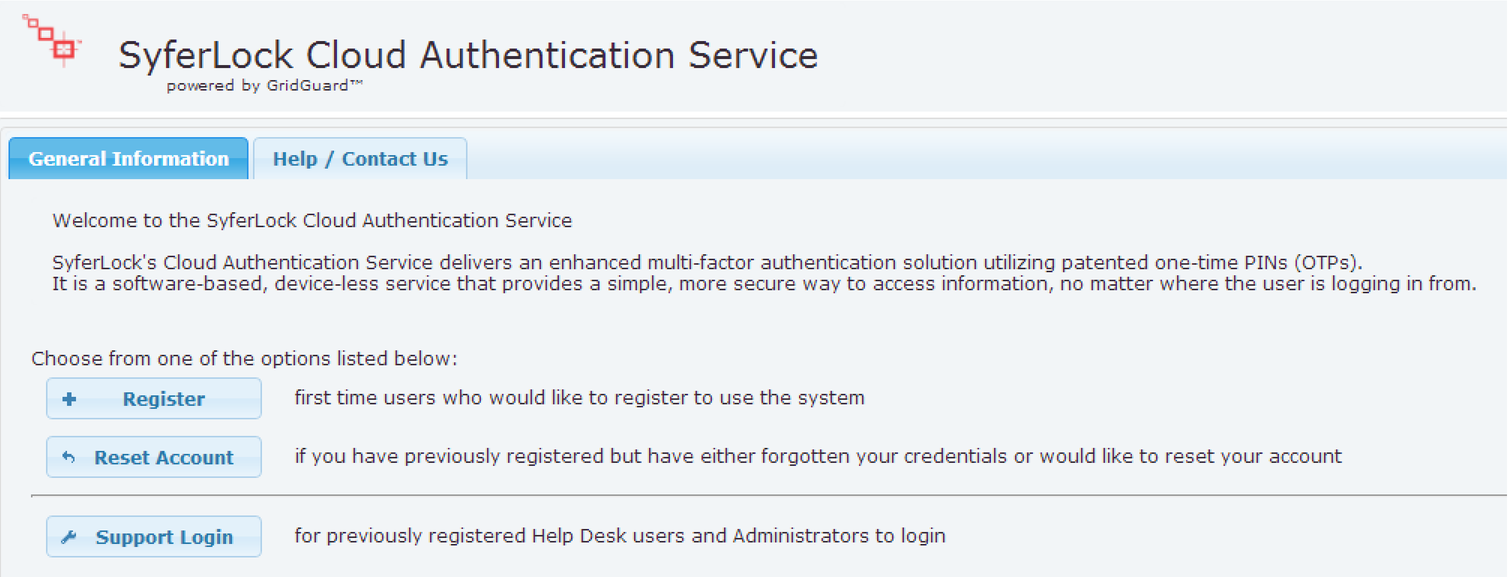
1. User accesses enrollment page and submits registration request with email address
2. System sends user an email which includes a one-time use enrollment token
3. User clicks on link in email to confirm ownership of email address
4. System prompts user to select PIN and target corner
5. User selects PIN and target corner
6. Registration is complete

Registration – Limited Enrollment


End User
Administrator
SyferLock GridGuard™ CAS
1
Create User
2
Send user enrollment email
3
User clicks on 'Complete Enrollment' link
4
Email address validated. User asked to select PIN and target corner
5
User selects PIN and target corner
6
Registration complete

1. Administrator creates an account for the user
2. System sends user an email which includes a one-time use enrollment token
3. User clicks on link in email to confirm ownership of email address
4. System prompts user to select PIN and target corner
5. User selects PIN and target corner
6. Registration is complete

SyferLock CAS Portal



SyferLock Cloud Authentication Service

powered by GridGuard™

Welcome to the SyferLock Cloud Authentication Service

SyferLock's Cloud Authentication Service delivers an enhanced multi-factor authentication solution utilizing patented one-time PINs (OTPs).
It is a software-based, device-less service that provides a simple, more secure way to access information, no matter where the user is logging in from.

Choose from one of the options listed below:

first time users who would like to register to use the system

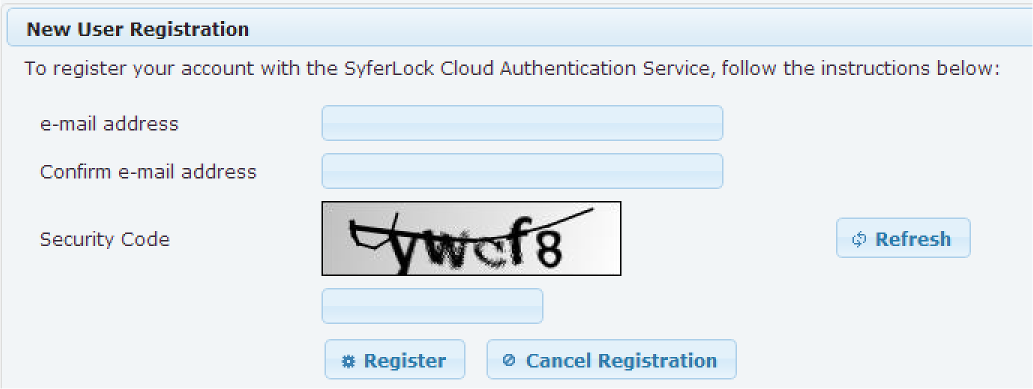
if you have previously registered but have either forgotten your credentials or would like to reset your account

for previously registered Help Desk users and Administrators to login

- CAS Portal
  - Allows first time users to register (Available only if the account has been setup for open enrollment)
  - Allows current users to reset their credentials
  - Allows Help Desk & Administrators to manage SyferLock CAS account

New User Registration

- Open Enrollment - User self-registers by providing email address



New User Registration

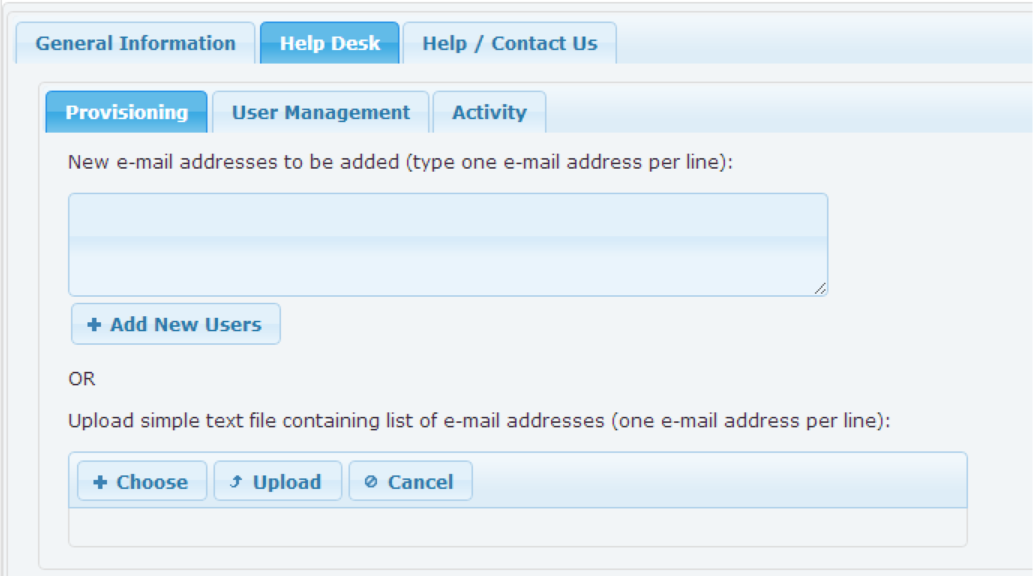
To register your account with the SyferLock Cloud Authentication Service, follow the instructions below:

e-mail address

Confirm e-mail address

Security Code

- Limited Enrollment – Administrator specifies list of users



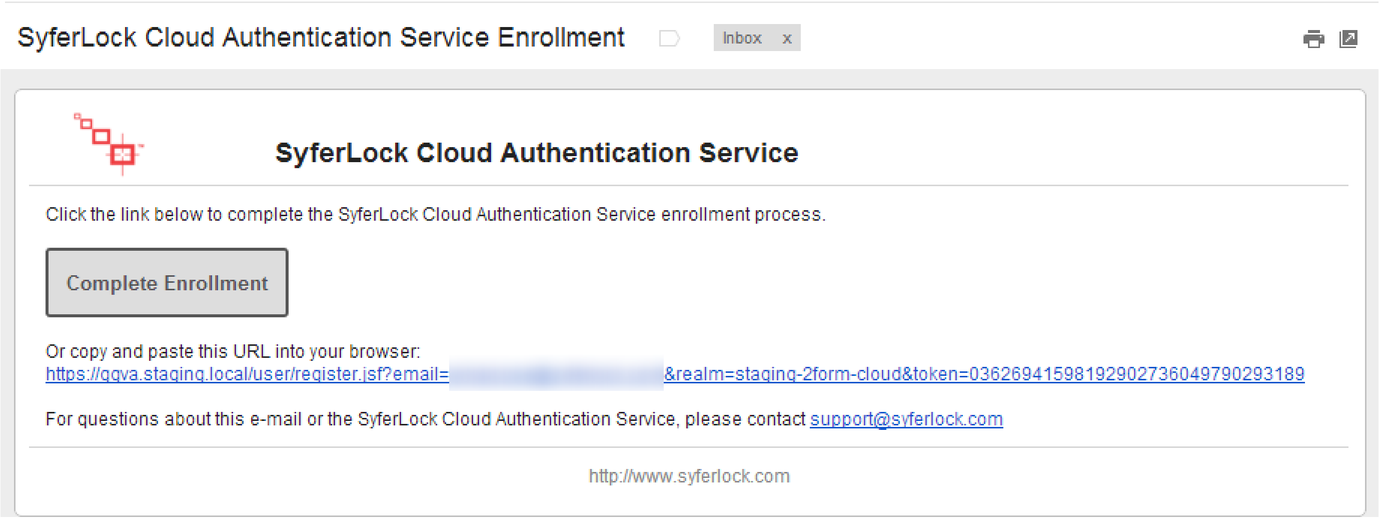
New e-mail addresses to be added (type one e-mail address per line):

OR

Upload simple text file containing list of e-mail addresses (one e-mail address per line):

New User Registration

- User sent an email to continue enrollment process. User clicks on ‘Complete Enrollment’



SyferLock Cloud Authentication Service Enrollment

SyferLock Cloud Authentication Service

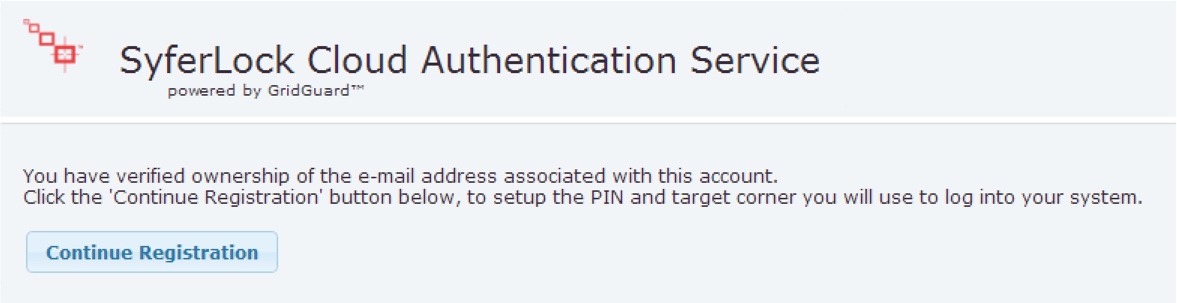
Click the link below to complete the SyferLock Cloud Authentication Service enrollment process.

Or copy and paste this URL into your browser:
https://qgva.staging.local/user/register.jsf?email=[redacted]&realm=staging-2form-cloud&token=03626941598192902736049790293189

For questions about this e-mail or the SyferLock Cloud Authentication Service, please contact support@syferlock.com

http://www.syferlock.com

- User account ownership verified. User clicks on ‘Continue Registration’

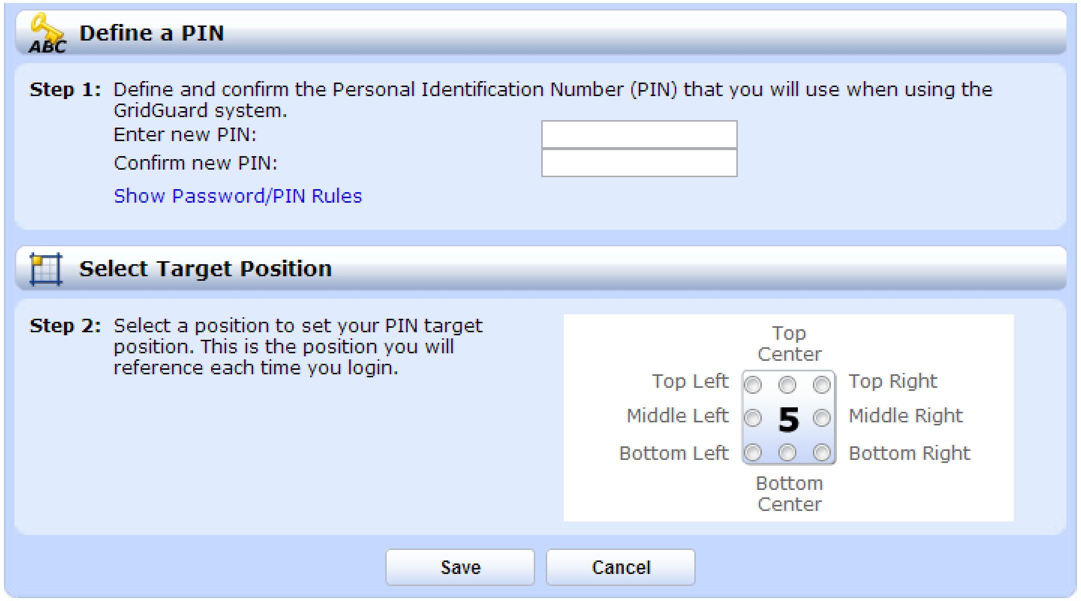


SyferLock Cloud Authentication Service
powered by GridGuard™

You have verified ownership of the e-mail address associated with this account.
Click the 'Continue Registration' button below, to setup the PIN and target corner you will use to log into your system.

New User Registration (Open Enrollment)

- User selects PIN and target corner



Define a PIN

Step 1: Define and confirm the Personal Identification Number (PIN) that you will use when using the GridGuard system.

Enter new PIN: ______

Confirm new PIN: ______

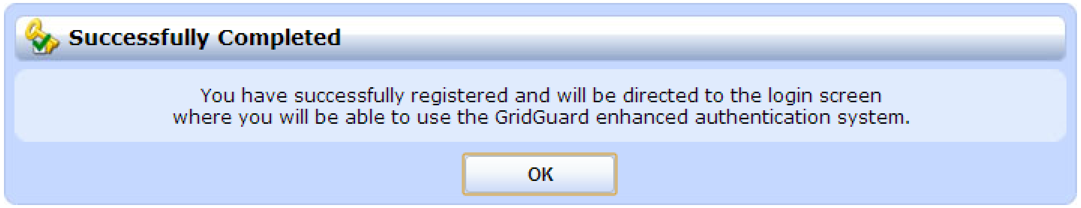
Show Password/PIN Rules

Select Target Position

Step 2: Select a position to set your PIN target position. This is the position you will reference each time you login.

		Top Center		
Top Left	○	○	○	Top Right
Middle Left	○	5	○	Middle Right
Bottom Left	○	○	○	Bottom Right
		Bottom Center		

- Registration Complete !!

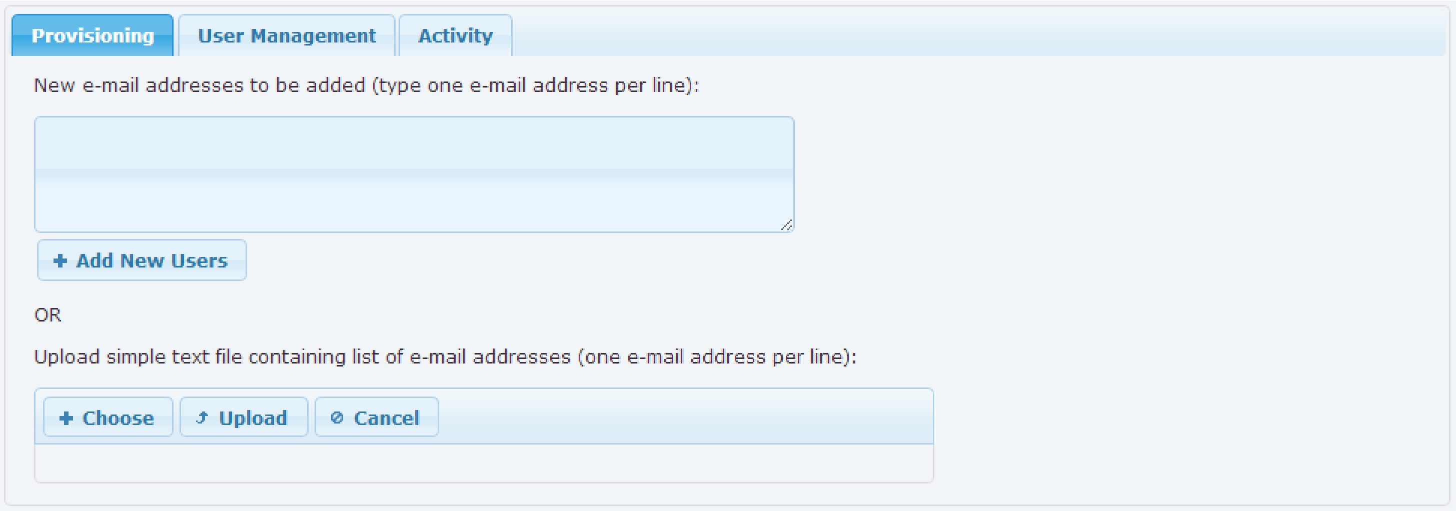


Successfully Completed

You have successfully registered and will be directed to the login screen where you will be able to use the GridGuard enhanced authentication system.

Help Desk Portal

- User Provisioning in two ways
  - Typing a list of users
  - Uploading a file containing a list of valid email addresses



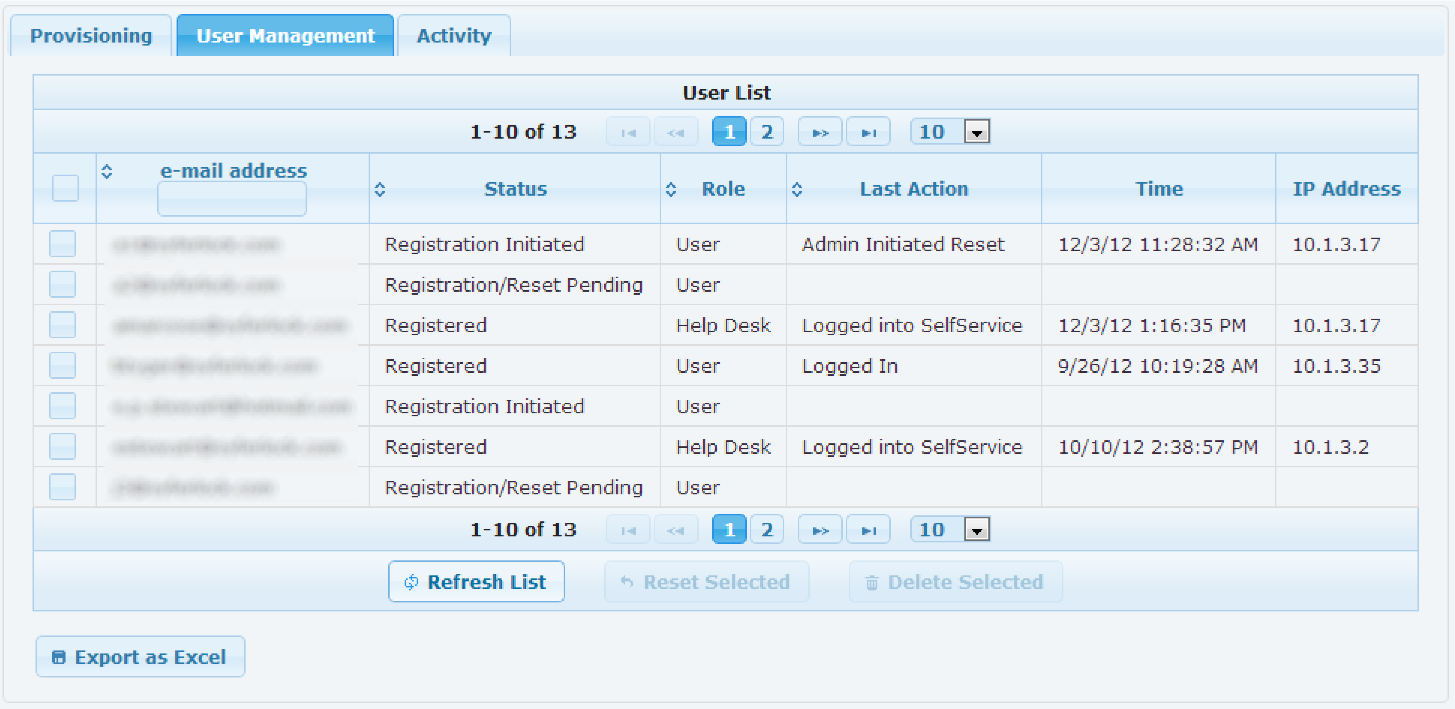
New e-mail addresses to be added (type one e-mail address per line):

OR

Upload simple text file containing list of e-mail addresses (one e-mail address per line):

Help Desk Portal

- User Management
  - View / Search list of registered users
  - Reset & Delete users
  - Export list of registers users as an Excel spreadsheet



User List

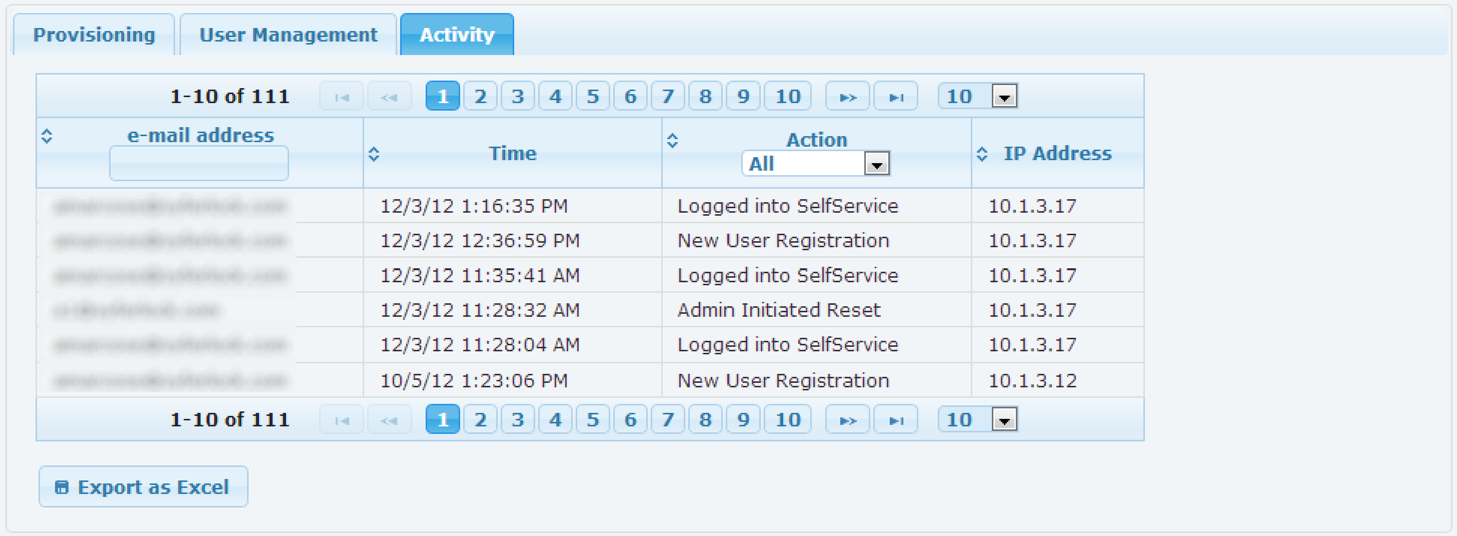
1-10 of 13

□	e-mail address	Status	Role	Last Action	Time	IP Address
□	[redacted]	Registration Initiated	User	Admin Initiated Reset	12/3/12 11:28:32 AM	10.1.3.17
□	[redacted]	Registration/Reset Pending	User			
□	[redacted]	Registered	Help Desk	Logged into SelfService	12/3/12 1:16:35 PM	10.1.3.17
□	[redacted]	Registered	User	Logged In	9/26/12 10:19:28 AM	10.1.3.35
□	[redacted]	Registration Initiated	User			
□	[redacted]	Registered	Help Desk	Logged into SelfService	10/10/12 2:38:57 PM	10.1.3.2
□	[redacted]	Registration/Reset Pending	User			

1-10 of 13

Help Desk Portal

- User Activity
  - View detailed activity reports for all users
  - Filters to search by user e-mail address
  - Export data to Excel spreadsheet



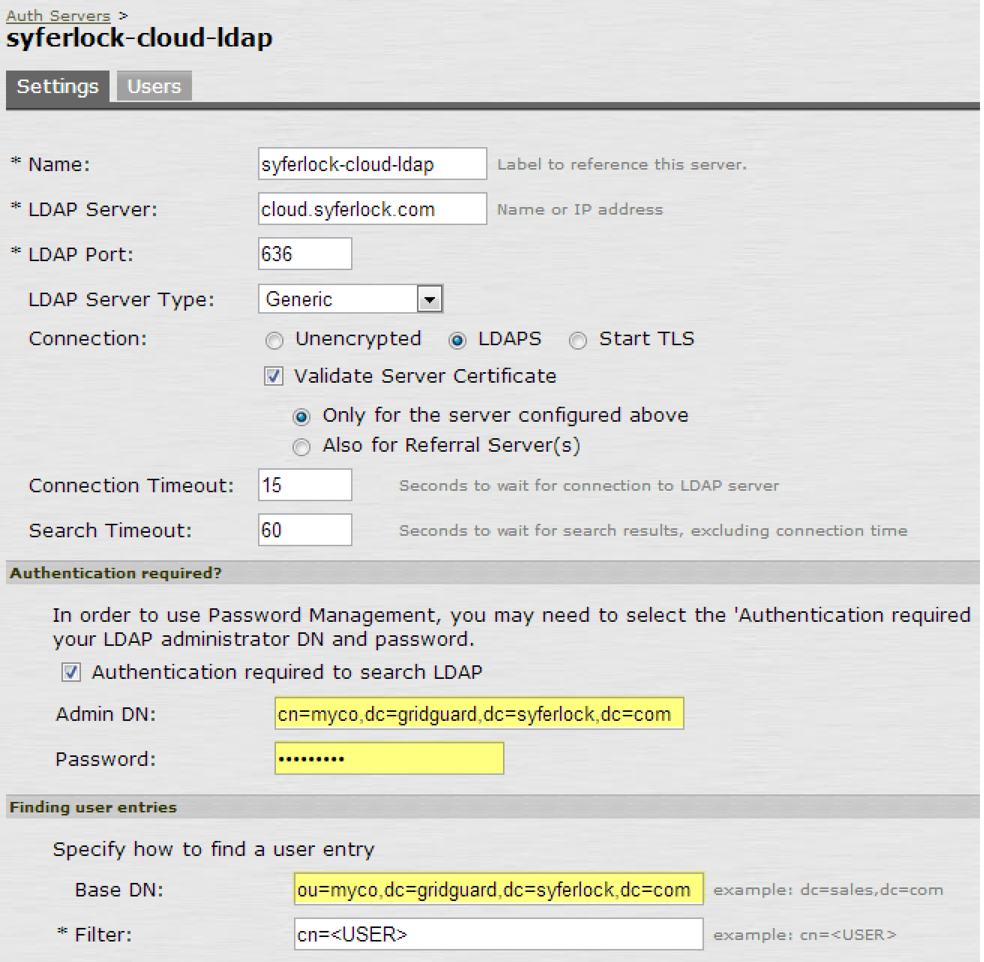
e-mail address	Time	Action All	IP Address
[redacted]	12/3/12 1:16:35 PM	Logged into SelfService	10.1.3.17
[redacted]	12/3/12 12:36:59 PM	New User Registration	10.1.3.17
[redacted]	12/3/12 11:35:41 AM	Logged into SelfService	10.1.3.17
[redacted]	12/3/12 11:28:32 AM	Admin Initiated Reset	10.1.3.17
[redacted]	12/3/12 11:28:04 AM	Logged into SelfService	10.1.3.17
[redacted]	10/5/12 1:23:06 PM	New User Registration	10.1.3.12

Sample Juniper SSL VPN Configuration

Setup Authentication Server

- Create an Authentication Server using the settings shown below:

  Admin DN, Password and Base DN (highlighted in yellow) will be specific to your account and provided to you by SyferLock



Auth Servers >

syferlock-cloud-ldap

Settings | Users

* Name:	syferlock-cloud-ldap	Label to reference this server.
* LDAP Server:	cloud.syferlock.com	Name or IP address
* LDAP Port:	636	
LDAP Server Type:	Generic	
Connection:	○ Unencrypted ● LDAPS ○ Start TLS	
	☑ Validate Server Certificate	
	● Only for the server configured above ○ Also for Referral Server(s)	
Connection Timeout:	15	Seconds to wait for connection to LDAP server
Search Timeout:	60	Seconds to wait for search results, excluding connection time

Authentication required?

In order to use Password Management, you may need to select the 'Authentication required your LDAP administrator DN and password.

☑ Authentication required to search LDAP

Admin DN:	cn=myco,dc=gridguard,dc=syferlock,dc=com
Password:	•••••••••

Finding user entries

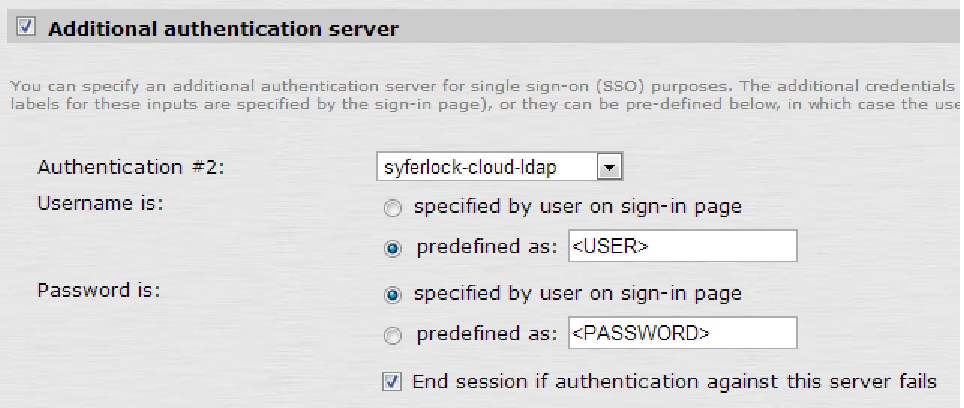
Specify how to find a user entry

Base DN:	ou=myco,dc=gridguard,dc=syferlock,dc=com	example: dc=sales,dc=com
* Filter:	cn=<USER>	example: cn=<USER>

Sample Juniper SSL VPN Configuration

Setup User Realm & Sign-In Page

- Configure User Realm to use SyferLock Cloud Authentication Server (syferLock-cloud-ldap) as the ‘Additional Authentication Server’



☑ **Additional authentication server**

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials labels for these inputs are specified by the sign-in page), or they can be pre-defined below, in which case the use

Authentication #2: syferlock-cloud-ldap

Username is: ○ specified by user on sign-in page ● predefined as: <USER>

Password is: ● specified by user on sign-in page ○ predefined as: <PASSWORD>

☑ End session if authentication against this server fails

- Import provided template file to create a custom sign-in page
- Create a sign-in URL to access the User Realm using the custom sign-in page
- Manage your account by logging in as an administrator at https://cloud.syferlock.com
- That’s it !!!

SyferLock™

for more information, contact us at
info@syferlock.com

SyferLock Technology Corporation
917 Bridgeport Avenue
Shelton, CT 06484 USA
www.SyferLock.com