



SyferLock GridGuard Authentication Solution

Integration With

CyberArk Privileged Account Security

SyferLock Technology Corporation

www.syferlock.com

GridGuard™ Two-Factor & Multi-Factor Authentication Solution

GridGuard Virtual Appliance Release v5.4.4 Build 18384 or greater

December 12, 2016

Table of Contents

Overview.....	3
Document Purpose.....	3
Prerequisites.....	5
Assumptions, Environments & Versions.....	5
SyferLock GridGuard™ Virtual Appliance Setup....	6
Configure External Authentication Server.....	6
Customer User Store Setup.....	9
GridGuard User Store & User Info Store Setup.....	11
Realm Configuration.....	14
GridGuard SAML Configuration.....	20
CyberArk Setup.....	23
Configuration Details.....	23
Restart the CyberArk PVWA.....	25
Testing.....	27
Create a Test User.....	27
Test User Registration.....	28
Test User Login Success.....	34
Test User Login Failure.....	39

Overview

Document Purpose

The purpose of this document is to provide instructions for integrating SyferLock's patented software-based two-factor and multi-factor authentication solutions using SyferLock's GridGuard Virtual Appliance with CyberArk's Privileged Account Security solution via SAML. This includes the specific details for modifying the CyberArk Privileged Account Security settings and the Syferlock GridGuard Virtual Appliance settings to allow their integrated communication for two-factor and multi-factor authentication.

CyberArk Privileged Account Security - Overview



CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world's leading companies to protect their highest value information assets, infrastructure and applications. Designed from the ground up for security, the CyberArk Privileged Account Security Solution provides the most comprehensive solution for on-premises, cloud and ICS environments. This complete enterprise-ready Privileged Account Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.

SyferLock GridGuard™ Authentication Solutions Overview



SyferLock (www.syferlock.com) provides an innovative software-based alternative to hard tokens, smart cards and other authentication solutions. SyferLock delivers two-factor & multi-factor authentication utilizing patented software-based grids to convert static passwords/PINs into token-less one-time passwords/PINs (OTPs). Increasingly, enterprises are turning to SyferLock and its software-based authentication solutions to strengthen security, eliminate hardware tokens and reduce Total Cost of Ownership (TCO).

SyferLock's GridGuard is deployed as a virtual appliance in the enterprise network and integrates with the existing user registry to provide seamless user registration and authentication to SSL VPN appliances, Identity & Access Management platforms, Privileged Access platforms, web portals, and cloud-based and other applications.

SyferLock Integrated With CyberArk

SyferLock's GridGuard software-based two-factor and multi-factor authentication solutions now provide a strong access control to the CyberArk's Privileged Account Security solutions, without the need for hardware tokens and without cell phone dependency like SMS-based solutions.

Prerequisites

Assumptions, Environments, & Versions

This document assumes that both a standard CyberArk Privileged Account Security installation and SyferLock GridGuard Virtual Appliance installation are already completed. This document was created and tested against the CyberArk PAS v9.7 and SyferLock GridGuard Virtual Appliance Release v5.4.4 Build 18384.

CyberArk Privileged Account Security

- CyberArk PAS v9.7

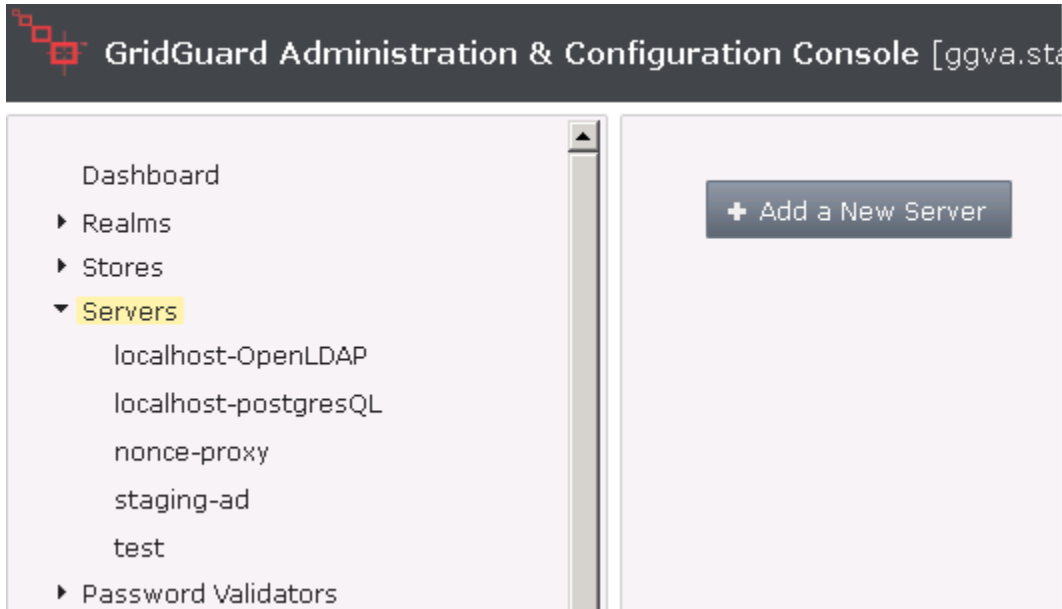
SyferLock GridGuard Virtual Appliance

- GridGuard Virtual Appliance Release v5.4.4 Build 18384 or greater
- LDAP based user storage (ex. Active Directory / OpenLDAP)

SyferLock GridGuard Virtual Appliance Setup

Configure External Authentication Server

Adding an Active Directory authentication server.



First, an authentication server for Active Directory must be configured.

Browse to the GridGuard Administration & Configuration Console (ACC). Click on 'Servers' to add a new authentication server. Then click on the 'Add a New Server' in the right side column.

Configure Active Directory

Server - New

Server ID:

Server Type: **LDAP** (dropdown)

LDAP Type: **External - Generic** (dropdown)

LDAP Server:

Ignore SSL Errors: ☐

Bind DN:

Bind Password:

Test User DN:

User Query:

User Attribute:

User Image Attribute:

Password Attribute:

Password Format: ☒ SSHA ☐ Plain Text

User Properties:

External Password Attribute:

Additional Attributes:

+ Add Server Update Server Test LDAP Connection Test DB Connection

Enter an authentication server label in the Server ID. Then select the Server Type as 'LDAP'.

Enter the appropriate configuration data for your Active Directory configuration.

- LDAP Type: External - Active Directory
- LDAP Server: Hostname of LDAP server in URI format, i.e. <ldaps://ad.company.com:636/>

If you are using secure LDAP, make sure you have imported your trusted Root certificates into GridGuard-VA. If you have imported the certificate, check the 'Ignore SSL errors' check box.

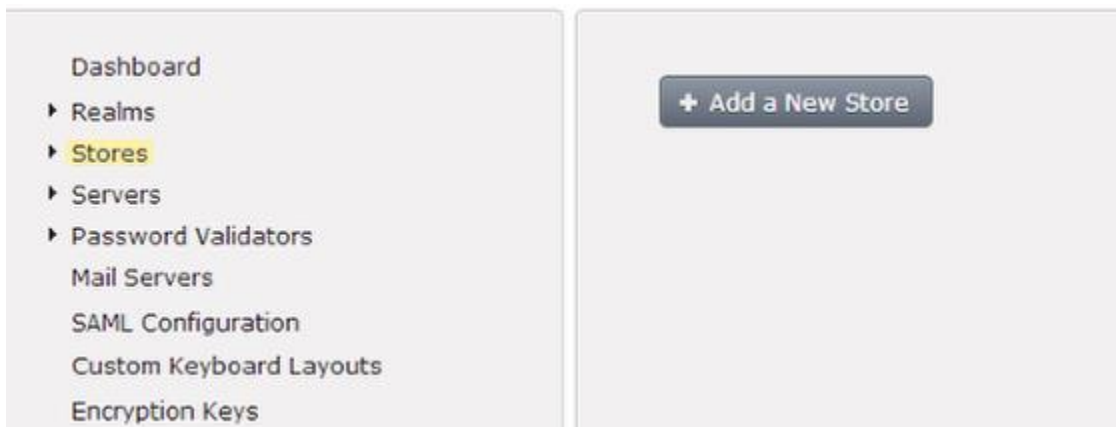
- Bind DN: Active Directory Service Account in Distinguished Name format. i.e. cn=Administrator,cn=Users,dc=example,dc=com
- Bind Password: Password associated with Bind DN account
- Test User DN: Leave blank
- User Query: Leave as default
- User Attribute: Leave as default
- User Image Attribute: Leave as default
- Password Attribute: Leave as default
- Password Format: Leave as default
- User Properties: Leave as default
- External Password Attribute: Leave as default
- Additional Attributes: cn, mail, memberOf (one per a line)

Click 'Add Server'. Click 'Test DB Connection' to validate the LDAP settings. Then click 'Apply Changes' to save the server to the configuration file.

Customer User Store Setup

This section provides instructions on how to configure the GridGuard server (virtual appliance) to access the customer's reference user store (typically Active Directory) for validating user passwords and group memberships.

Choose 'Add a New Store' option



Choose **Stores** > **Add a New Store**

Create User Store Reference

Configuration Console [ggva-load-1.staging.local]

Store - New

Store ID

Store Type

Storage Type

LDAP Server

Base DN

+ Add Store

Apply Changes **Revert Changes**

Enter a name for the store that will be created (e.g. testuserstore)

Valid store types include:

- **Gridstore** - Where the generated valid grids are stored
- **Historystore** - Where the user history is stored (i.e. logins, user account changes)
- **Sessionstore** - Where sessions are stored
- **Noncestore** - Where nonces are stored in a nonce-based implementation
- **Userstore** - Database of record for user lookup
- **Userinfostore** - Where all the GridGuard specific data is stored

Type of storage used to store the data

- **Memory** - data stored in RAM
- **Database** - data stored in a JDBC supported database (e.g. mssql)
- **LDAP** - data stored on an LDAP server
- **Custom** - data stored in a custom-defined storage environment

ID of the LDAP server associated with this store

Define the LDAP server in DistinguishedName format (e.g. dc=testserver, dc=local)

1. Set **Store ID** to a unique name that will be used to identify this user store
2. Set **Store Type** to **userStore**
3. Set **Storage Type** to **LDAP**
4. Set **LDAP Server** to the name of the assigned to the server created above
5. Set **Base DN** to the base dn that will be used to query for users on this server
6. Click **Add Store**
7. Click **Apply Changes** to save all changes

GridGuard User Store & User Info Store Setup

This section provides instructions on how to setup a GridGuard user store and a GridGuard user info store.

The user store is the store against which lookups are performed to determine if the user is a registered user of the system; the user info store is used to store the PIN, corner/target position and GridPic associated with the user. Typically, these are stored on the GridGuard server (virtual appliance) in the same LDAP OU.

The GridGuard server (virtual appliance), by default, comes with a user store (DefaultRealm-2Form-UserStore) and a user info store (DefaultRealm-2Form-UserInfoStore) pre-configured. If you are using the pre-configured stores, you can skip the steps below completely.

Follow the steps below only if you want to use a separate LDAP OU to store the user credentials for this integration.

Create a new LDAP OU

The screenshot shows the GridGuard Administration & Configuration Console [ggva-load-1.staging.local]. The left sidebar contains a navigation menu with the following items: Dashboard, Realms, Stores, Servers, Password Validators, Mail Servers, SAML Configuration, Custom Keyboard Layouts, Encryption Keys, License & User Management, Certificates, Radius Setup, **LDAP Configuration** (highlighted with a red circle and number 1), Page Customizations, Service Management, Backups & Restores, and Cluster Management. The main content area has three tabs: General, LDAP Proxy, and **LDAP User Org. Unit (OU)** (highlighted with a red circle and number 2). Below the tabs is a section titled 'User Organizational Unit (OU) Configuration' containing a table with two rows of OUs and their Distinguished Names (DNs). The first row is 'ou=defaultRealm,dc=gridguard,dc=syferlock,dc=com' and the second is 'ou=test,dc=gridguard,dc=syferlock,dc=com'. Each row has a 'Delete' button. Below the table is a '+ Add User OU' button (highlighted with a red circle and number 3). A modal dialog box titled 'Add User OU' is open, showing a text input field for 'OU Distinguished Name (DN)' (highlighted with a red circle and number 4) and two buttons at the bottom: '+ Add User OU' (highlighted with a red circle and number 5) and 'Cancel'.

1. Choose the **LDAP Configuration** option
2. Click on the **LDAP User Org. Unit (OU)** tab
3. Click **Add User OU**
4. A new dialog window is displayed. Enter the DN (short name) of the OU to create
5. Click **Add User OU**

This will create a new user OU that will be used to store user information.

Create User Store Reference

Configuration Console [ggva-load-1.staging.local]

Store - New

Store ID

Store Type

Storage Type

LDAP Server

Base DN

+ Add Store

Enter a name for the store that will be created (e.g. testuserstore)

Valid store types include:

- **Gridstore** - Where the generated valid grids are stored
- **Historystore** - Where the user history is stored (i.e. logins, user account changes)
- **Sessionstore** - Where sessions are stored
- **Noncestore** - Where nonces are stored in a nonce-based implementation
- **Userstore** - Database of record for user lookup
- **Userinfostore** - Where all the GridGuard specific data is stored

Type of storage used to store the data

- **Memory** - data stored in RAM
- **Database** - data stored in a JDBC supported database (e.g. mssql)
- **LDAP** - data stored on an LDAP server
- **Custom** - data stored in a custom-defined storage environment

ID of the LDAP server associated with this store

Define the LDAP server in DistinguishedName format (e.g. dc=testserver, dc=local)

Apply Changes **Revert Changes**

1. Set **Store ID** to a unique name that will be used to identify this store
2. Set **Store Type** to **userStore**
3. Set **Storage Type** to **LDAP**
4. Set **LDAP Server** to **localhost-OpenLDAP**
5. Set **Base DN** to the base DN of the OU created in the step above

Create User Info Store Reference

Configuration Console [ggva-load-1.staging.local] Apply Changes Revert Changes

Store - New

Store ID

Store Type userinfoStore

Storage Type LDAP

LDAP Server localhost-OpenLDAP

Base DN

+ Add Store

Enter a name for the store that will be created (e.g. testuserstore)

Valid store types include:

- **Gridstore** - Where the generated valid grids are stored
- **Historystore** - Where the user history is stored(i.e logins, user account changes)
- **Sessionstore** - Where sessions are stored
- **Noncestore** - Where nonces are stored in a nonce-based implementation
- **Userstore** - Database of record for user lookup
- **UserinfoStore** - Where all the GridGuard specific data is stored

Type of storage used to store the data

- **Memory** - data stored in RAM
- **Database** - data stored in a JDBC supported database (e.g mssql)
- **LDAP** - data stored on an LDAP server
- **Custom** - data stored in a custom-defined storage environment

ID of the LDAP server associated with this store

Define the LDAP server in DistinguishedName format (e.g. dc=testserver, dc=local)

1. Set **Store ID** to a unique name that will be used to identify this store
2. Set **Store Type** to **userinfoStore**
3. Set **Storage Type** to **LDAP**
4. Set **LDAP Server** to **localhost-OpenLDAP**
5. Set **Base DN** to the base DN of the OU created in the step above

Realm Configuration

General Tab

Configuration Console [] Apply Changes Undo Changes

Realm - New

General | Grid Options | Cryptographic Options | 2-factor Options | Fields | User Groups | URLs | Stores | Advanced

Realm Name Enter desired realm name

Corners Number of corners to display in each Grid cell

Grid Mode Grid Modes

- **GridAdvanced**: a one-to-many mapping of characters to corner elements (cryptograms).
- **GridBasic**: a one-to-one mapping of characters to corner elements.

Process type Process Type is used to tell the GridServer how to handle the login process

- **Generic**- for generic configurations
- **Connectra**- for Connectra devices
- **Cookie Capture**- used where the GridServer logs in as user and forwards the cookie to the browser
- **Custom**- for configurations where a custom class is used for handling login process
- **Juniper**- for all Juniper installations
- **Netscaler**- for Netscaler devices
- **OWA2010**- for Outlook Web Access 2010
- **Repost**- directly reposts user password to login page (should only be used when no other option is available)
- **SAML**- for all SAML deployments
- **Symplified**- for integrating with Symplified
- **Token Authentication**- for LDAP enabled backends to generate a nonce (preferred method if possible, unless a specific device is shown)

Process type specific parameters

Name	Value	Options
No records found.		
+ Add		

Specific parameters used for the process type. See documentation for required parameters

- Realm Name: Realm Identifier
- Corners/Target Positions : Select number of cell corners/target positions
- Grid Mode: GridAdvanced
- Process Type: SAML

Grid Options Tab

Realm - ADFS

General Grid Options Cryptographic Options 2-factor Options Fields User Groups URLs Stores Advanced

2Form Options

Enable 2Form ☒ Enables Grid2Form, where the user password is passed along with a GridPIN to the backend server

Enable GridPIN ☒ Enables GridPIN. Used in conjunction with Grid2Form, but can also be used with numeric passwords as well

Device configuration 2 authentication servers Number of authentication servers defined in the target system configuration

Nonce content PIN Set to 'Password' to encrypt password within nonce; set to 'PIN' to encrypt pin within nonce

Authenticate with PIN only? ☐ If checked, authentication will be performed using PIN only; if unchecked, both password and PIN will be required for authentication.

Other Options

Enable MyGrid ☐ Enables the user to select from a list of layout options

Force Layout To pin Forces the user layout to a specified value

Enable Password Change ☒ Enables the user to change their password for the backend Active Directory or LDAP server (only enable if the service account has appropriate rights)

Enable Number Pad ☒ Enable entry via a clickable numpad

Enable GridPic ☒ Enables the GridPic functionality, allowing users to upload a personal photo

GridPic Required ☐ Requires a GridPic during registration

Require DialIn Access ☐ Requires Dial-in Access (Active Directory only)

Default Image Default image to be used as GridPic when user does not specify one

Grid Timeout 180 Specify the timeout for grids, in seconds. Typically 180 -

2Form Options

- Enable 2Form : Checked
- Enable GridPIN: Checked
- Device Configuration: Use "2 Authentication Servers" for 2Form. Use "1 Authentication Server" for PIN only.
- Nonce Content: PIN
- Authenticate with PIN Only: Check if you are using PIN Only

Other Options

- Enable My Grid: Uncheck
- Force Layout: PIN
- Enable Password Change:
- Enable Number Pad:
- Enable GridPic:

Cryptographic Options Tab

All of the options here can be set to any reasonable setting.

2-Factor Options Tab

All of the options here can be set to any reasonable setting.

Fields Tab

The screenshot shows a configuration window titled "Realm - SAML_2Form". Inside, there is a tabbed interface with the following tabs: General, Grid Options, Cryptographic Options, 2-factor Options, and Fields. The "Fields" tab is selected and highlighted in blue. Below the tabs, there are four rows of configuration options, each with a label, an input field, and a description:

Label	Input Field	Description
Username Field	username	HTML input field name that contains the user's primary username
Username Field #2		HTML input field name that contains the user's secondary username. Used only in 2form configurations
Password Field		HTML input field name that contains the user's primary password
Password Field #2		HTML input field name that contains the user's secondary password. Used only in 2form configurations

- Username Field : "username"
- Password Field : <blank>

User Groups Tab

All of the options here can be set to any reasonable setting.

URLs Tab

Realm - ADFS

General	Grid Options	Cryptographic Options	2-factor Options	Fields	User Groups	URLs	Store
Restricted HTTP Referer List						Ente acct One Ex. http	
Base URL						Ente loca sett imp	
Authentication URL						Ente auth is u: sett imp	
Landing URL						Ente redi auth they This imp	
Logout URL	%REFURL%					Ente whe	
Login Failed URL	%REFURL%					Ente whe succ	
Locked Out URL	%REFURL%					Ente whe	
IP Lookup Site	<input "="" type="text" value="http://ws.arin.net/whois/?queryinput="/>					The the Cen see	

- Restricted HTTP Referer List : <Set appropriately>
- Base URL : <Only needs to be set if GridSoftToken is enabled.>
- Authentication URL : <BLANK>
- Landing URL : <BLANK>
- Logout URL : %REFURL%
- Login Failed URL : %REFURL%
- Locked Out URL : %REFURL%
- IP Lookup Site : <Leave as is>

Stores Tab

Realm - ADFS

General	Grid Options	Cryptographic Options	2-factor Options	Fields	User Groups	URLs	Stores	Advanced
Grid Store	gridStore						The store where generated grids are stored	
History Store	historyStore						The store where activity logs are stored	
Primary User Store	DefaultRealm-2Form-UserStore						The store where the user's primary credential is stored. In 2form configurations, the grid credential is always considered the primary. When 2form is enabled, this should be the store used to store the grid credential (typically, a store on the gridguard server itself). When 2form is not enabled, it should be the store used to store the 1 credential being validated. When unchecked, the username as entered by the user is used in the repost template. If checked, the user identity value is used instead of the username. For LDAP based user stores, the user identity value will be the DN; for databases, this may be an identity column defined for the user record.	
Username is UserID	☐							
Secondary User Store	staging-ad-userstore						The secondary store where user information is stored. In 2form configurations, the grid credential is always considered the primary. This should be the store used to store the external credentials (typically, an external LDAP/AD server).	Secondary User Store staging-ad-userstore initialized with warnings
Userinfo Store	DefaultRealm-2Form-UserInfoStore						The store where GridPass (corner, layout etc.) information is stored	
Nonce Store							This store where the nonce is stored. This is usually a LDAP server	
Session Store							The store where temporary user session information is	

- Grid Store : Select a valid grid store.
- History : Select a valid history store.
- Primary User Store : User store associated with GridGuard.
- Username is UserID: Unchecked
- Secondary User Store: User Store associated with Active Directory.
- User Info Store : User Info store associated with GridGuard.
- Nonce Store : <BLANK>
- Session Store : Select a valid session store.

Advanced Tab

Realm - ADFS

General	Grid Options	Cryptographic Options	2-factor Options	Fields	User Groups	URLs	Stores	Advanced
Enable Self-registration	☐							Allow self-registration of users to realm
Proxy Header Field								HTTP Header field containing proxy address information (e.g X-Forwarded-For)
Pass Authentication to Backend	☒							Always authenticate to backend system, passing bad authentication requests to enforce lockout policies
ClickJacking Protection	☒							Enables anti-ClickJacking protection. Will NOT allow pages to be run within iframes. Disable this option if this is required
Enable Debug Mode	☐							Enables various debug tools (additional submit buttons, etc)
Disable Login Button	☐							Disable the login button. Used for access to Security Center only

- Enable Self-registration : Set Appropriately
- Proxy Header Field : Set Appropriately
- Pass Authentication to Backend : Checked
- ClickJacking Protection : Checked
- Enable Debug Mode : Unchecked
- Disable Login Button : Unchecked

GridGuard SAML Configuration

Set up the SAML values for GridGuard that will be relevant for the CyberArk Integration

SAML Configuration - General Tab

GridGuard Administration & Configuration Console [] Apply Changes Undo Changes Logout

General | Login Page Settings | Reference URLs

ServiceProvider - CyberArk

Signing Certificate: 4 SGVA-Demo-2016 3

Import SP Metadata: + Choose Upload Cancel

Import SP Metadata URL: Go

Entity ID: 5 PasswordVault

ACS URL: 6 https://127.0.0.1/PasswordVault

Assertion Configuration

Validity Time:

Enable SSO: ☒

SSO Timeout:

Realm: 7 SAML_2Form

Name Identifier: 8 sAMAccountName

Name ID Type: 9 unspecified

Sign Assertion: 10 ☒

Encrypt Assertion: ☐

Attribute Mapping

Name	Value
No records found.	

+ Add Attribute Mapping

11

1. Right Click on SAML Configuration in the left pane
2. Choose Add
3. Name the SAML Configuration
4. Pick a Cert for the Signing Certificate, make a note of the Signing Certificate that you selected
5. For the EntityID put PasswordVault
6. Add the ACS URL <https://<PasswordVault FQDN>/PasswordVault>
7. Choose the SAML_2Form Realm you created
8. Choose sAMAccountName as the Name Identifier

9. Choose unspecified as the Name ID Type
10. Check the Sign Assertion Checkbox
11. Click Apply Changes

SAML Configuration - Reference URL Tab

The screenshot displays the GridGuard Administration & Configuration Console interface. The left sidebar contains a navigation menu with the following items: Dashboard, Realms, Stores, Servers (expanded), Demo-AD-2Form-Proxyed, Demo-AD-Adv-Proxyed, GridDemo.Internal, localhost-OpenLDAP, localhost-OpenLDAP-Proxyed, localhost-mysql, nonce-proxy, Password Validators, Mail Servers, SMS Providers, and SAML Configuration (expanded). Under SAML Configuration, the following providers are listed: ADFS, NetScaler10, OpenAM, Okta, XenMobile, NetScaler10-NSAuth, NetScaler10-CitrixReady-2Form, SalesForce-1, OPENIAM, and CyberArk (highlighted in yellow).

The main content area shows the 'Reference URLs' tab selected. It contains four input fields for SAML configuration:

- SP initiated login URL:** A text input field with a circled '1' next to it, containing the URL `https://[redacted]/saml/idp`.
- IdP initiated login URL:** A text input field containing the URL `https://[redacted]/saml/initiate/CyberArk`.
- Logout URL:** A text input field containing the URL `https://[redacted]/saml/logout/CyberArk`.
- Metadata URL:** A text input field containing the URL `https://[redacted]/saml/md/CyberArk`.

At the top right of the console, there are two buttons: 'Apply Changes' and 'Undo Changes'.

Copy the SP initiated login URL

Copy the Logout URL.

SAML Configuration - Retrieve PEM CERT

GridGuard Administration & Configuration Console [REDACTED] [Apply Changes](#) [Undo Changes](#) [Logout](#)

Dashboard

- Realms
- Stores
- Servers
- Password Validators
- Mail Servers
- SMS Providers
- SAML Configuration** 3
 - ADFS
 - NetScaler10
 - OpenAM
 - Okta
 - XenMobile
 - NetScaler10-NSAuth
 - NetScaler10-CitrixReady-2Form
 - SalesForce-1

Identity Provider (IdP) Configuration

Hostname Fully qualified GridGuard server domain name (FQDN) as seen by the service provider. For e.g., grid.company.com

IdP Certificates			
Label	Issuer	Export	Options
Default Certificate	SyferLock - Demo - DefaultSAML Cert	PEM ↓	i x
GridGuard-Demo-RSA	GridGuard-Demo-RSA	PEM ↓	i x
GGVA-Demo-2016	GGVA-Demo-2016	PEM ↓ 4	i x
FullFQDN		PEM ↓	i x

[Import PKCS12](#) [Generate New Certificate](#)

Export Certificate

Export Certificate 5 Export Certificate

1. In the Left Pane, Single Click the Header "SAML Configuration"
2. Click the Export (Download Arrow) for the Cert you picked in the General Tab Settings
3. Click the Download Button in the Export Certificate Window that is presented.
4. Locate the "samlCertificate.pem" file that is downloaded.
5. Open in an editor.
6. Stripe out everything except for the cert, including the line breaks, until you have a solid line of just the cert.

CyberArk Setup

Configuration Details

The following instructions were taken from the CyberArk's document "Privileged Account Security Implementation Guide".

Configuring Access through the PVWA

The screenshot shows the 'System Configuration' page in the CyberArk PVWA. The 'ADMINISTRATION' tab is selected. In the left sidebar, 'Authentication Methods' is expanded, and 'saml' is selected. The 'Properties' table on the right lists the following configuration details:

Name	Value
Id	saml
DisplayName	SyferLock/SAML
Enabled	Yes
MobileEnabled	No
LogoffUrl	https://[redacted]gridguard/saml/logout/CyberArk
UseVaultAuthentication	No
UseRadius	No
UseLDAP	No
SignInLabel	
UsernameFieldLabel	
PasswordFieldLabel	

Below the table, the 'AuthMethod' section is visible, stating: 'AuthMethod Defines an authentication method.' At the bottom right, there are buttons for 'Apply', 'OK', and 'Cancel'.

Log onto the PVWA as the predefined Administrator user.

Click ADMINISTRATION to display the System Configuration page

Click Options

The main system configuration editor appears.

Expand Authentication Methods; a list of the supported configuration methods is displayed.

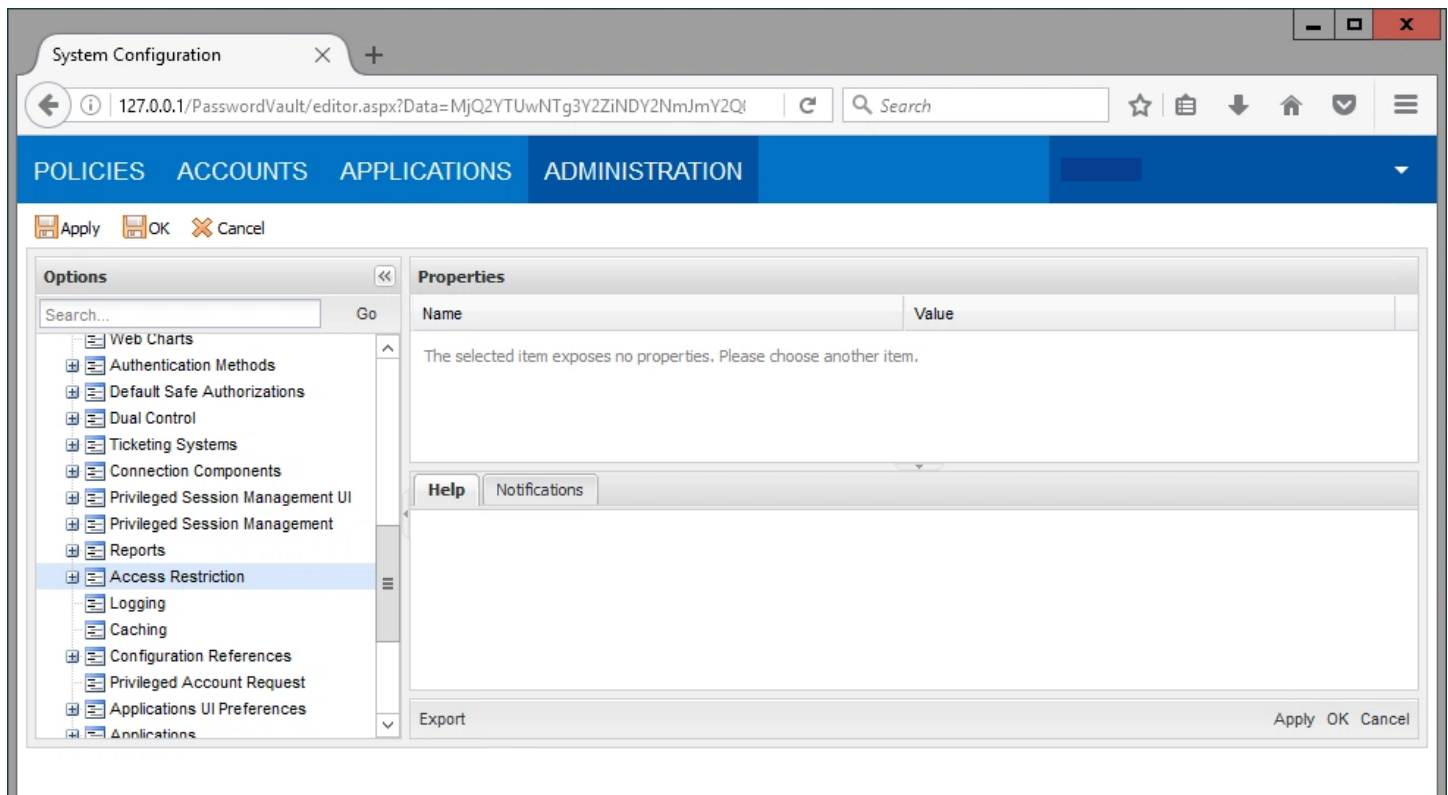
Specify the following Authentication Methods properties

Select SAML and make sure the Enabled property is set to Yes.

In LogoffUrl, specify <https://<SyferlockApplianceAddress>/gridguard/saml/logout/CyberArk>

Click Apply to save the new configurations and stay in the Options page, or, Click Save to save the new configurations and apply them after the period of time specified in the RefreshPeriod parameter.

Configuring PVWA SAML Authentication



In the PVWA:

1. In the Options page, right-click Access Restriction, then select Add AllowedReferrer; a new parameter node is added to enable you to configure an Allowed Referrer.
2. In the Allowed Referrer property list, in BaseURL, specify:
<https://<Syferlock Appliance Address>/gridguard/saml/idp>
3. Click Apply to save the new configurations.

Configuring Web.config SAML Authentication

In the PasswordVault web.config file

1. In the PasswordVault installation folder, open the web.config file. Default Location:
C:\inetpub\wwwroot\PasswordVault\
2. In the appSettings tag, add the following mandatory parameters:
 - IdentityProviderLoginURL:https://<Syferlock Appliance Address>/gridguard/saml/idpIdentityProviderCertificate – The base 64 text representation of the certificate that is configured for your Syferlock Appliance as the SAML response signing certificate. This is used by the PVWA to verify the authenticity of the responses.

```
<appSettings>
  [...]
  Rest of the appSettings
  [...]
  <add key="IdentityProviderLoginURL" value="https://[... SP initiated
login URL ...]/gridguard/saml/idp"/>
  <add key="Issuer" value="PasswordVault"/>
  <add key="IdentityProviderCertificate" value="[... The stripped down
Certificate ...]"/>
</appSettings>
```

Restart the CyberArk PVWA

After the completion of the update to the Web.config file, restart the IIS running **iisreset** /**restart** as Administrator.

Change to the Web.config file should cause the PVWA application to reinitialize automatically.

Testing

Create a Test User

Create a Test User in AD

Add a user in the LDAP store using the normal processes.

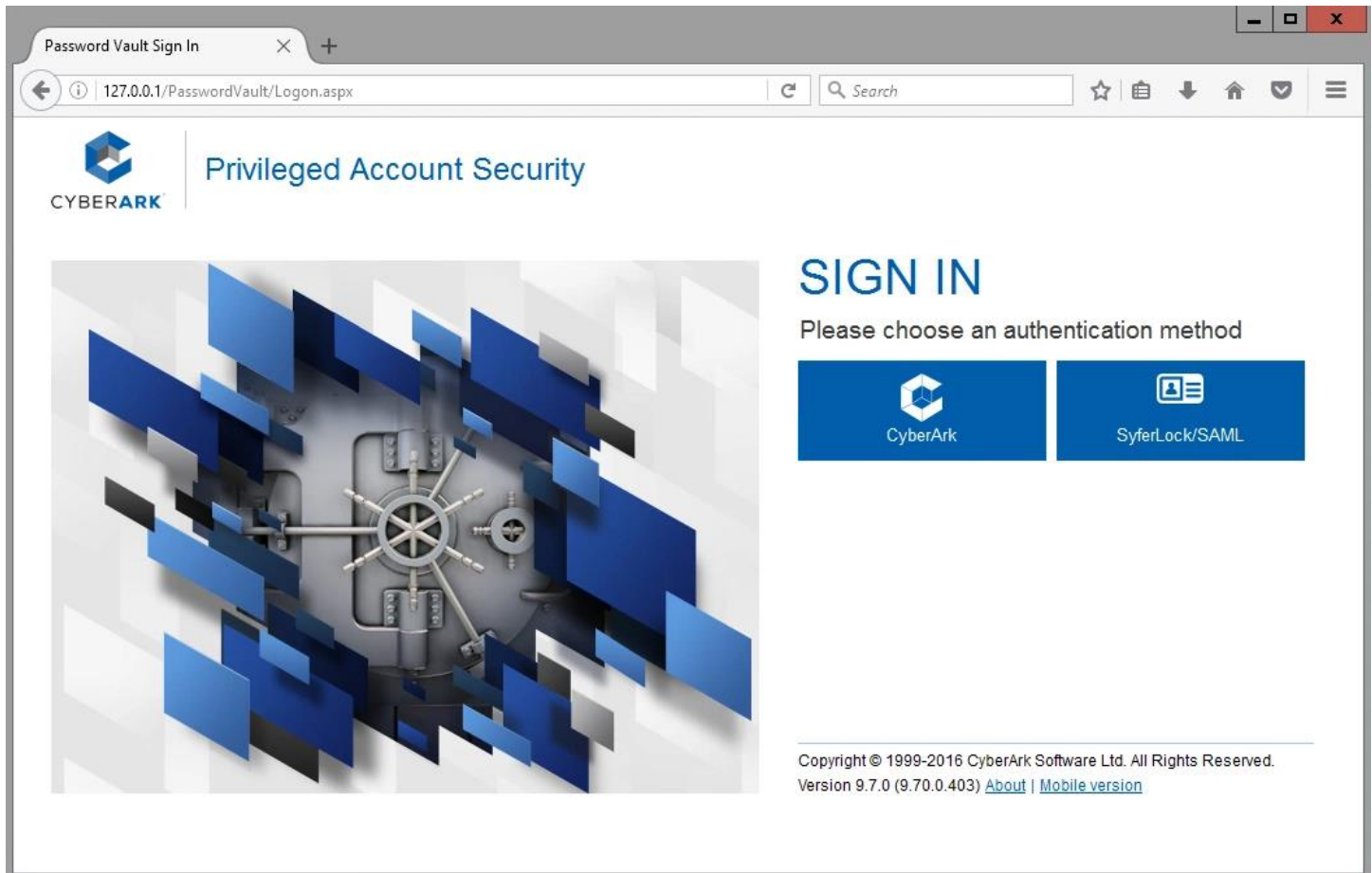
Create a Test User in CyberArk

Use the instructions in the CyberArk Privileged Account Security Installation Guide

Test User Registration

Test User Registration

On the PVWA



Click the SyferLock SAML Tile

SyferLock SAML Login Page

https://ggva.demo.syferlock.com/gridguard/saml/idp?SAMLRequest=fZFPb4MwDMW%

SyferLock GridGuard™ Login

Your company has implemented a new enhanced login system. This system will provide you with secure one-time password authentication.

Please enter ONLY your username

Username:

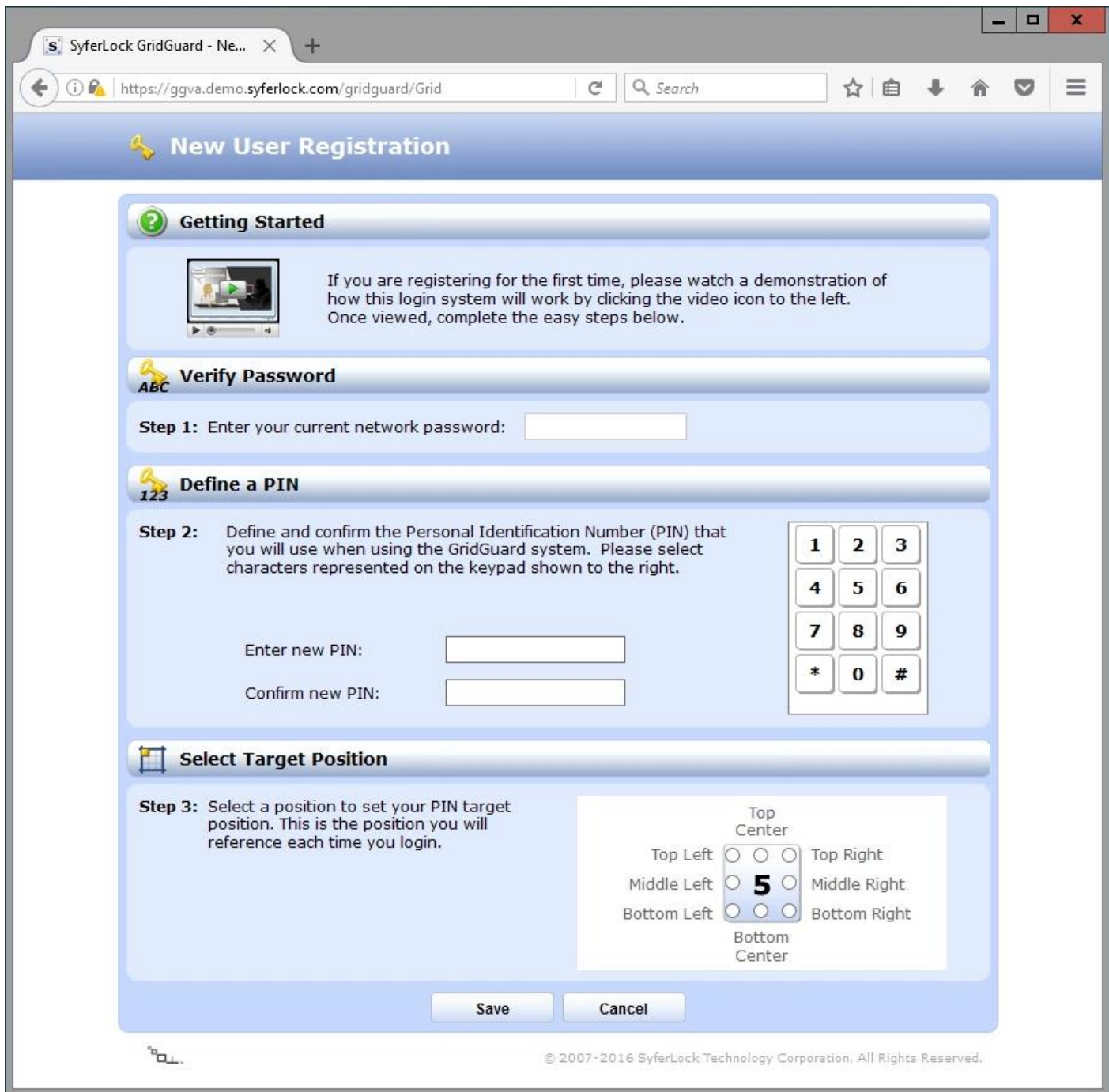
[Login](#)
secured by grid

Enter username and click login to continue

All Rights Reserved © 2007 - 2016, SyferLock Technology Corporation

Enter the correct UserID

Click Login



SyferLock GridGuard - Ne... X

https://ggva.demo.syferlock.com/gridguard/Grid

New User Registration

Getting Started

If you are registering for the first time, please watch a demonstration of how this login system will work by clicking the video icon to the left. Once viewed, complete the easy steps below.

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:

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

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.

	Top Center	
Top Left	☐	Top Right
Middle Left	☒	Middle Right
Bottom Left	☐	Bottom Right
	Bottom Center	

Save **Cancel**

© 2007-2016 SyferLock Technology Corporation, All Rights Reserved.

The Registration page will display

Enter your Network Password.

Select your PIN & Corner/Target Position

SyferLock GridGuard - Ne... X

https://ggva.demo.syferlock.com/gridguard/Grid

New User Registration

Getting Started

 If you are registering for the first time, please watch a demonstration of how this login system will work by clicking the video icon to the left. Once viewed, complete the easy steps below.

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:

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

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.

	Top Center	
Top Left	☐	Top Right
Middle Left	☐	Middle Right
Bottom Left	☐	Bottom Right
	Bottom Center	

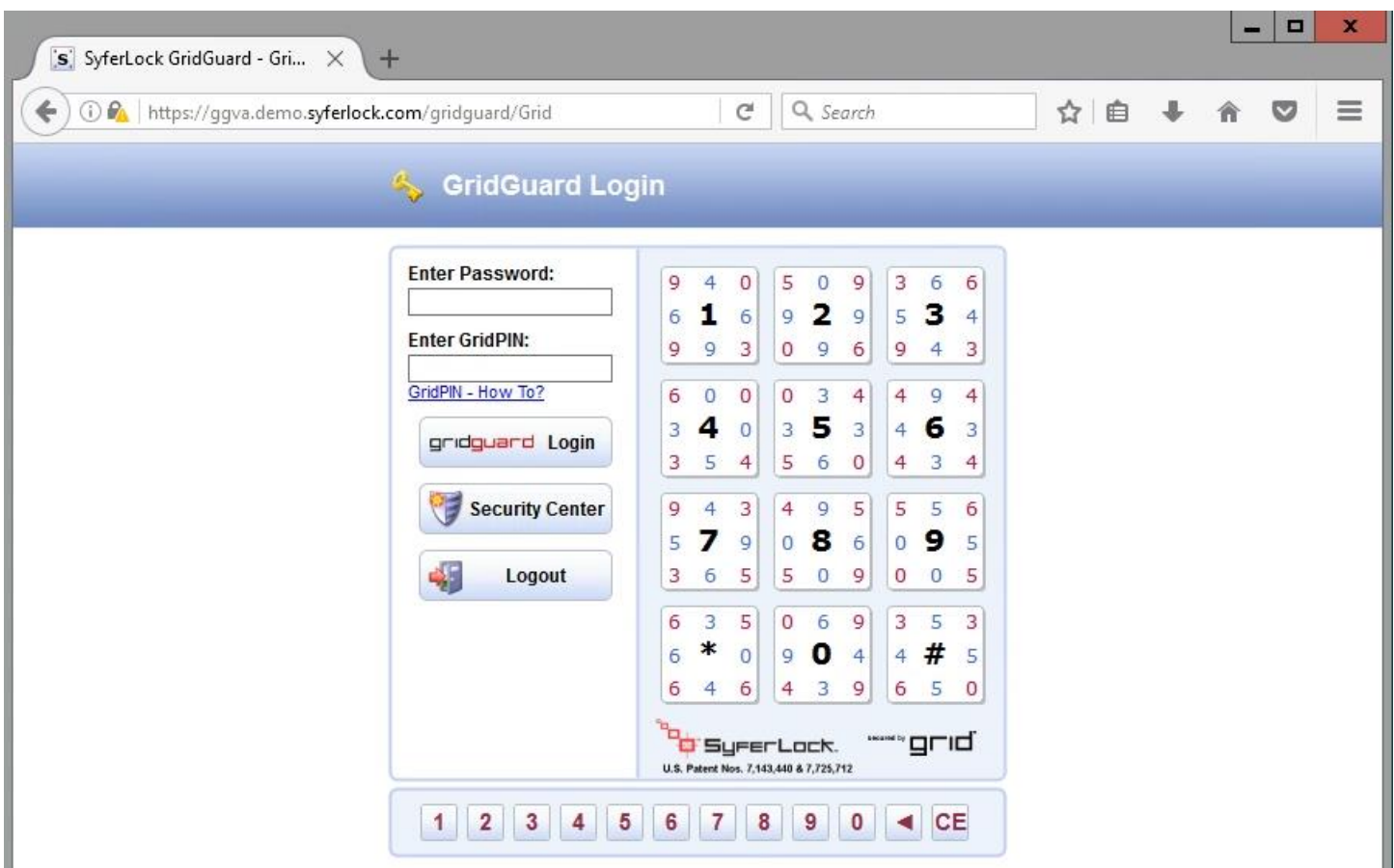
© 2007-2016 SyferLock Technology Corporation, All Rights Reserved.

Click Save



Registration will indicate success

Click OK to Proceed to Login



Enter your Network Password

Determine GridPIN using your PIN + Corner/Target Position and the Provided Grid

Click the Login button

Recently

127.0.0.1/PasswordVault/myaccounts.aspx?Data=XkBeXkBeMF5AXI5...

POLICIES ACCOUNTS APPLICATIONS ADMINISTRATION estewart

ACCOUNTS

R... [Add SSH Key](#) [Add Account](#) [Customize](#) [Search](#)

[Request Access](#) [Manage](#) [Modify](#) [Add to](#) [Detect Now](#)

☐	Username	Address	Safe	Platform ID					
--------------------------	----------	---------	------	-------------	--	--	--	--	--

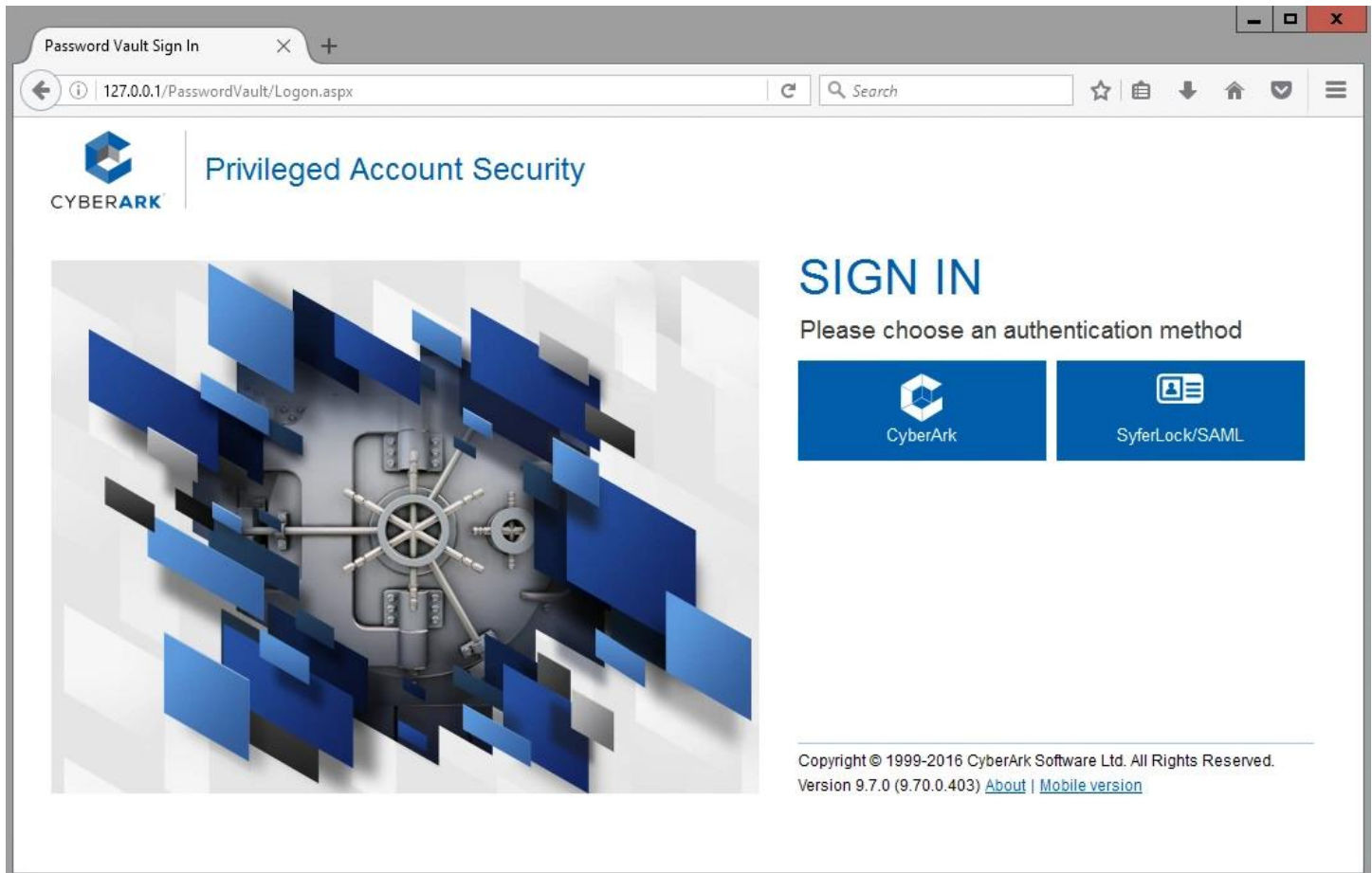
127.0.0.1/PasswordVault/myaccounts.aspx?Data=XkBeXkBeMF5AXI5AXI5AXjBeQF5GYWxzZV5AXI5AXkhY2tVUkw9TXNnRXJyPU1zZ0luZm89 No accounts to display

The user should be logged into the CyberArk Password Vault.

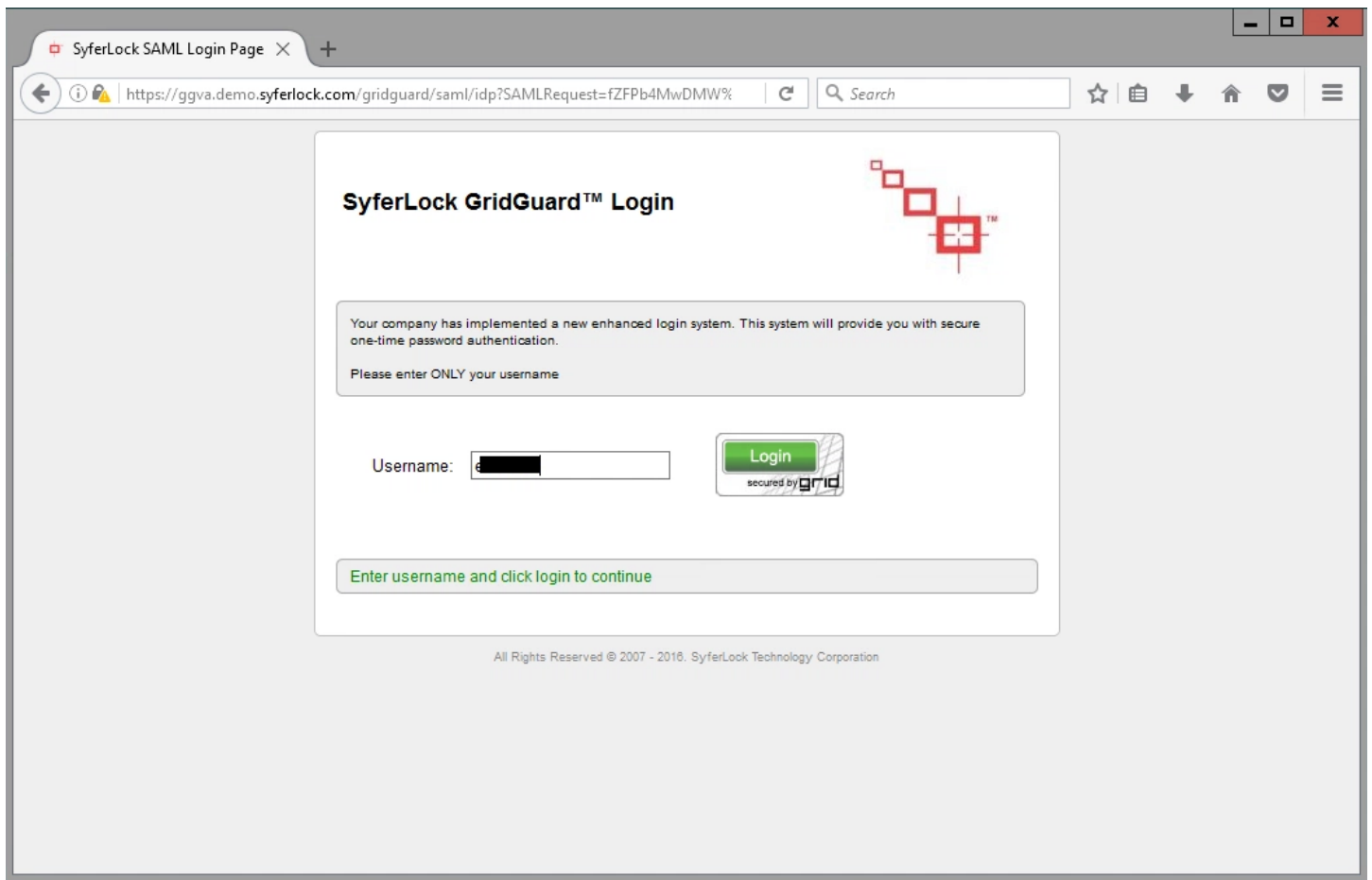
Test User Login Success

Test User Login Success

In the PVWA



Click the SyferLock SAML Tile



The screenshot shows a web browser window with the title "SyferLock SAML Login Page". The address bar displays the URL: <https://ggva.demo.syferlock.com/gridguard/saml/idp?SAMLRequest=fZFPb4MwDMW%>. The page content includes the "SyferLock GridGuard™ Login" header with a logo of three red squares. A message box states: "Your company has implemented a new enhanced login system. This system will provide you with secure one-time password authentication. Please enter ONLY your username". Below this is a "Username:" label followed by a text input field containing a redacted value. To the right of the input field is a green "Login" button with the text "secured by grid" underneath. A green instruction bar at the bottom of the form reads "Enter username and click login to continue". The footer of the page contains the text: "All Rights Reserved © 2007 - 2016, SyferLock Technology Corporation".

SyferLock SAML Login Page

https://ggva.demo.syferlock.com/gridguard/saml/idp?SAMLRequest=fZFPb4MwDMW%

SyferLock GridGuard™ Login

Your company has implemented a new enhanced login system. This system will provide you with secure one-time password authentication.

Please enter ONLY your username

Username:

Login
secured by grid

Enter username and click login to continue

All Rights Reserved © 2007 - 2016, SyferLock Technology Corporation

Enter the correct UserID

Click Login

SyferLock GridGuard - Gri... X +

https://ggva.demo.syferlock.com/gridguard/Grid

GridGuard Login

Enter Password:

Enter GridPIN:

[GridPIN - How To?](#)

gridguard Login

Security Center

Logout

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

SyferLock. grid
 U.S. Patent Nos. 7,143,440 & 7,725,712

1 2 3 4 5 6 7 8 9 0 ◀ CE

Enter the Correct AD Password

Enter the GridPIN that corresponds to the previously selected PIN and Corner/Target Position

SyferLock GridGuard - Gri... X +

https://ggva.demo.syferlock.com/gridguard/Grid

GridGuard Login

Enter Password:
.....

Enter GridPIN:
...

[GridPIN - How To?](#)

gridguard Login

Security Center

Logout

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

 **SyferLock** U.S. Patent Nos. 7,143,440 & 7,725,712 

1 2 3 4 5 6 7 8 9 0 ◀ CE

Click Login

The screenshot shows a web browser window with the URL `127.0.0.1/PasswordVault/myaccounts.aspx?Data=XkBeXkBeMF5AXI5AXI5AXjBeQF5GYWxzZV`. The application has a blue header with tabs: **POLICIES**, **ACCOUNTS**, **APPLICATIONS**, and **ADMINISTRATION**. The user `estewart` is logged in. The left sidebar shows the **ACCOUNTS** section expanded, with **Recently (0)** selected. The main content area is titled **Recently** and contains buttons: **Add SSH Key**, **Add Account**, **Customize**, and a search bar. Below these are buttons: **Request Access**, **Manage**, **Modify**, **Add to**, and **Detect Now**. A table header is visible with columns: **Username**, **Address**, **Safe**, and **Platform ID**. The status bar at the bottom indicates **No accounts to display**.

The user should be granted access to the Vault.

Test User Login Failure

Test Registered User Failure

Test Login with a Valid UserID & Invalid Password

Login should fail

Test Login with a Valid UserID & Valid Password & Invalid GridPIN

Login should fail

Test Unregistered or Invalid User Failure

Test Login with Unregistered UserID & Invalid Password

Should show registration, but should fail the login

Test Login with an Invalid UserID

Should present "Dummy Grid" and fail login attempts

SyferLock Contact Information

Business Contact:

Chris Cardell
ccardell@syferlock.com
1-203-292-5441

Technical Contact:

Frank LaPlante
flaplante@syferlock.com
1-203-941-0575 x705

Support Contact:

support@syferlock.com
U.S. 1-855-793-3756 x2
Intl. 1-203-941-0575 x2