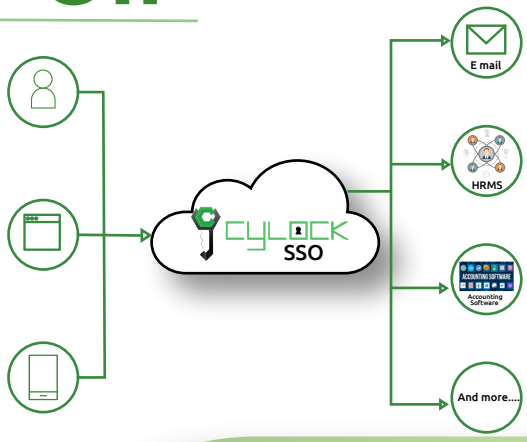
CyLock SSO

CYBERNEXA
Authentication Redefined

Single Sign-On

Single sign-on (SSO) is an authentication mechanism that allows a user to log in with a single user credential to multiple web applications (cloud or on-premises) and sites. CyLock Single Sign-On (SSO) solution is part of Cybernexa's identity suite of products, tailored for organizations embracing mobile and cloud technologies. Our solution is designed to meet user productivity objectives, mitigate security risks, compliance to regulatory requirements with reduced overhead costs. CyLock SSO can be used by enterprises, financial institutions, and governments to eliminate the need for managing multiple credentials for its user and customers. .



How Single Sign On Works?

Single sign-on is based on the concept of federated identity management in which one or more applications (service provider) have a trust relationship set with an SSO service (identity provider). When a user signs in to one of the applications the SSO service provider will check whether the user has already signed in. If an authentication token is available, then the same will be shared with the application. If not, a new token will be shared with the application. When the user tries to log in to any other application that has a mutual trust established with the SSO service, then they are automatically granted access. Standard SSO is achieved through federated protocols like OIDC, OAuth, and SAML 2.0.

SSO service need not necessarily store the user credentials. Most SSO services validate the user credentials against a separate identity management services like Active Directory (AD) or LDAP or other Identity Providers.

Benefits

- Enforce strong and realistic password policies.
- Eliminate the need to manage multiple passwords.
- Boost user productivity as they need to remember fewer passwords and sign in once.
- Protect access to any application - On-premise or cloud hosted.
- Defend against cyber-attacks.
- Reduced IT help desk calls for a password reset.
- Better visibility, tracking, and control of applications by the IT team.
- Compliance to regulatory requirements

SSO Capabilities & Features:

- **Unified Portal:** User friendly portal that can be used by administrators as well as end users to manage, monitor and configure user accounts, applications and security settings enabled with workflow options.

- **User Management:** Automatically synchronize data from Active Directory, OpenLDAP, FreeIPA and other LDAPs into SSO database for user provisioning and de-provisioning. Import data to SSO database when synchronization is not possible. Authenticate users against AD/LDAP, SSO database or against another IdP.

- **Identity Federation:** Core engine supports modern protocols like SAML, OAuth, OpenID, WS-Fed to facilitate federation to a wide range of applications and services.

- **Deployment Model:** Apart from the SaaS cloud deployment available for any organization to self-register for SSO; on-premise and private cloud deployments are also available.

- **Auditing & Reporting:** Fine grained auditing and real-time data reports enable IT administrators to promptly investigate and address any issues. Choose from a set of pre-built reports to gain a more comprehensive insight into how your end-users interact with applications and assess the presence of any potential security risks.

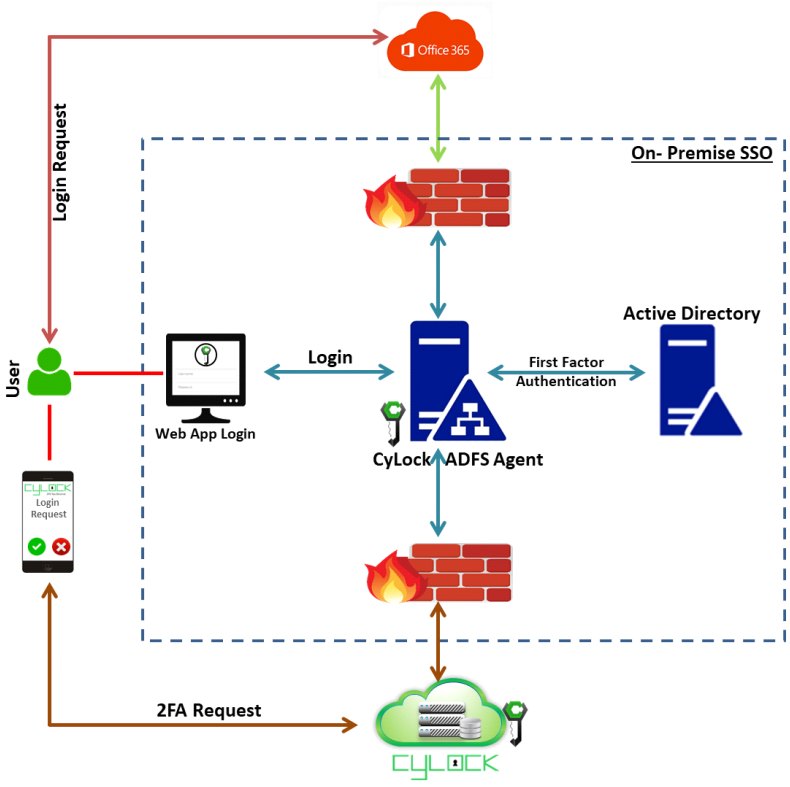
- **Strong Authentication:** On top of strong password policies, organizations can enable MFA to provide a more secure SSO process within the organization. MFA can provide security against cyber-attacks thereby safeguarding enterprise identity and data. With multiple MFA options, administrators can configure and trigger an MFA based on their risk requirements.

- **Browser Plug-in:** Cross-platform browser plug-in to enable Secure Browser Authentication for SSO to different applications.

Single Sign-On Strategies:

Considering the varying requirements of each organization, our SSO solution provides multiple ways through which SSO can be achieved.

1) Organizations using Microsoft Active Directory as the user store for all the applications can enable SSO through CyLock SSO ADFS agent. Both on-premises applications and Cloud services like O365 and Google Workspace can be enabled with SSO through this on-premises ADFS setup. The figure below shows a typical SSO flow using ADFS.



2) Integrated Windows Authentication (IWA) is a user authentication mechanism developed by Microsoft. IWA simplifies the login process for users accessing web applications that utilize Active Directory as a user store. In this mechanism, all a user has to do is log into their Windows domain. Once done they are automatically authenticated into any IWA enabled web applications. To increase the login security, organizations can use CyLock's Windows Credential Provider enabled with MFA for Windows logon.

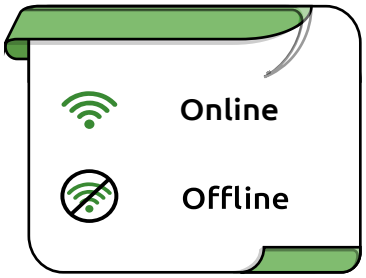
3) Our federation IdP engine can provide SSO for applications that can consume SAML protocol. Organizations can either user our SaaS version or deploy our solution on-premise to enable SSO for their applications

4) In case of organizations having multiple applications with its individual user store and different credentials, SSO like experience can be provided using Secure Browser Authentication (SBA) through our SaaS SSO deployment.

Built-in MFA :

CyLock platforms zero trust approach provides a strong and secured MFA during single sign-on. The table below lists the authentication types and the security options supported during SSO.

AUTHENTICATION		
MODE	TYPE	SECURITY
	Push	Push, Biometric, Pin
	QR	Biometric, Pin
	CR - OTP	Pin, Biometric
	CR - OTP, CR - OTP	Pin, Biometric
	POTP, POTP	None
	TOTP	None
	GRID	Pin



Summary :

Seamless and fast access to internal or external work applications without the need of remembering multiple passwords or logging into individual applications, will improve employee productivity. CyLock SSO enabled with strong security can make this happen by providing a smooth user experience.

To learn more about our product and how it can secure your applications, talk to our support team.

CYBERNEXA
Authentication Redefined

+91 8667069354
sales@cybernexa.com
www.cybernexa.com