CionSystems Cloud Identity Minder

Provides Self-Service, Strong Authentication, and User Life Cycle Management

General Information: **info@cionsystems.com**

Online Support: **support@cionsystems.com**

CionSystems Inc.
6640 185th Ave NE
Redmond, WA-98052, USA
http://www.CionSystems.com
Phone: +1.425.605.5325

Now you can adopt SaaS application without the need to provision or share Login IDs and passwords. CionSystems Cloud Identity Minder simplifies the deployment of SaaS applications by eliminating the need for complex provisioning and synchronization. Users authenticate using their preferred login, without exposing their password to external parties. CionSystems Cloud Identity Minder can be deployed as a cloud service, in intranet or extranet scenarios or hosted environment. Affordable and flexible pricing is available in both subscription, per use, and traditional licensing models.

CionSystems Cloud Identity Minder is a cloud or on-premises identity, authentication, self-service and user life cycle management solution. CionSystems Cloud Identity Minder integrates SaaS and on-premises applications, without the need for custom coding or synchronizing user names and passwords. You no longer need to add custom code for each Identity store. The solution provides self-service password reset, auditing, notification, workflow and more.

Applications are not dependent on a specific identity store. Applications and cloud services do not need to share user ID's or passwords. Identities stay within the confine of existing location (on premise or cloud). This speeds deployment, simplifies operations, reduces compliance overhead, and improves security. CionSystems Cloud Identity Minder can be deployed internally within the enterprise, in the DMZ, externally hosted or in the cloud.

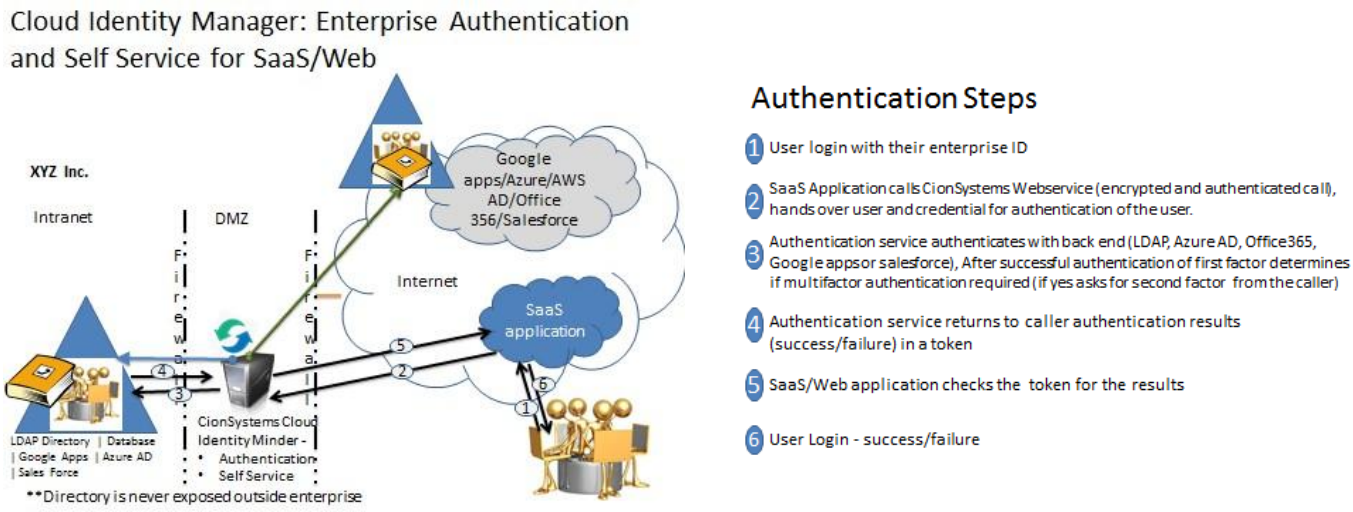

Figure 1.

Figure 1 Shows a typical DMZ deployment scenario. Here, CionSystems Cloud Identity Minder sits in the enterprise's DMZ. Typically, CionSystems Cloud Identity Minder does not require opening additional ports for authentication and access. For on-premises deployments, CionSystems Cloud Identity Minder can be hosted on standalone or domain joined systems. SaaS and Web applications call the CionSystems webservice to evaluate authentication requests. All communications are natively encrypted, so both http and https can be used securely. These simple and flexible options allow for easy deployment, supporting a wide variety of environments and use cases

The SaaS/Web application is unaware of the in the underlying identity store, or even how the user was authenticated. The authentication service validates the user and for the calling application. Note, the authentication service supports "step up authentication" via challenge questions, Out of Band notification (SMS, email, text to voice, soft tokens) and multifactor authentication. Additionally, the SaaS/Web application can embed the Self-service URL's, enabling self-enrollment for users. Users can reset their password, manage their profile, and perform other account management tasks.

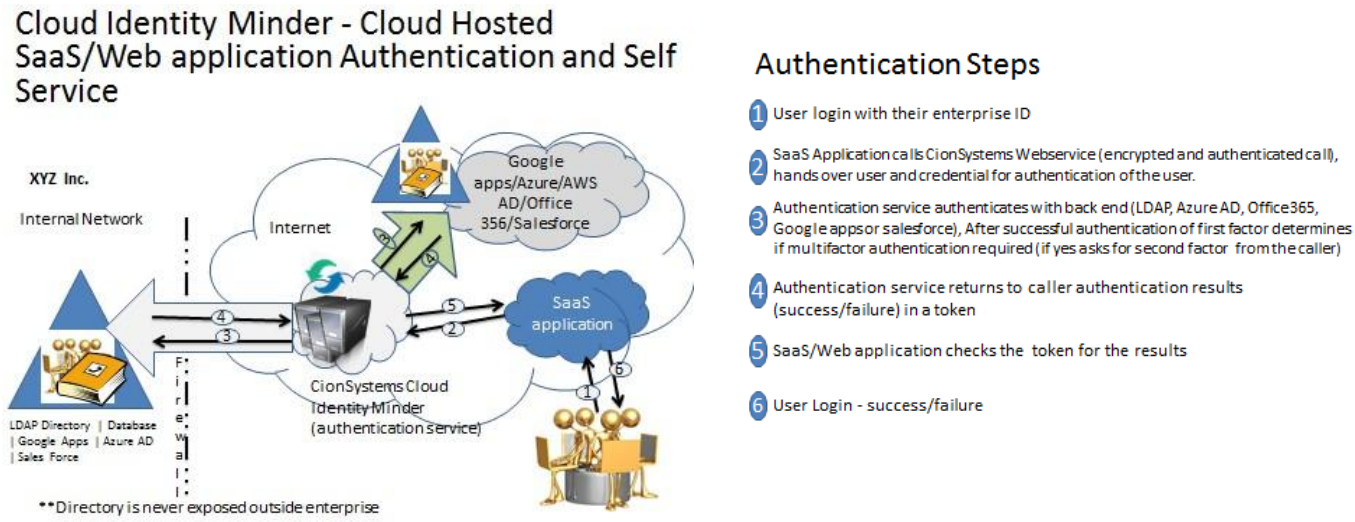

Figure 2

Figure 2 Shows a cloud hosted deployment. CionSystems Cloud Identity Minder is available as IaaS (Infrastructure as a Service), hosted, managed service, or cloud instance (Azure, AWS, or Private Cloud – others on request). In this scenario, ports are opened in the enterprise firewall to allow Authentication and Self-service can communicate with the back-end identity store via secure link. For additional security, CionSystems Cloud Identity Minder enforces endpoint address constraints, bolstering security.

SaaS and Web applications validate users via the cloud hosted CionSystems Cloud Identity Minder webservice using standard http or https protocol and ports. The session data is encrypted to enhance security and protect against compromised systems within the hosting environment. IPSec and VPN technology can also be used to add an additional layer of security. Endpoint restrictions protect against network based and denial of service attacks. Applications are not dependent on the underlying identity store, which is opaque and inaccessible to the calling application.

The authentication service validates the user and returns a token to the caller. Note, as above, step up authentication as well via challenge question, SMS, SMS via email and other factors is supported and all self -service abilities are available via the cloud.

CionSystems Cloud Identity Minder's multi factor authentication can be easily integrated with any web or non-web application. Instead of applications managing the strong authentication, developers can offload that functionality to CionSystems Cloud Identity Minder. In addition, this enhances applications' functionality and utility by providing end users with self-passwords reset, profile and account management, and powerful audit capabilities. This greatly reduces the help desk workload. (This functionality can be enabled per feature and per application, greatly enhancing security, consistency, and ease of use.) Users can securely manage their own profile data, so SaaS, internal and web- application need not implement and maintain these elements.

Self-Service can also send alerts and generate reports for:

- Locked Out Users
- Eminent Password Expiration for cloud base, on-premises, LDAP, domain, and other user credentials
- Password resets
- SaaS usage
- Expired User Passwords

Self-Service tracks all activity in an audit log that contains information such as who modified which passwords and when, and from what ip address. Users can update their own personal information (as determined by policy set by system administrators) without helpdesk intervention.

Service providers for billing can also use these reports. Enterprises can utilize the reports for governance, audit, and compliance purposes, as well as, to implement chargebacks and track overall usage.

Benefits	Features
Supports Microsoft Azure AD, Office 365, Microsoft AD, Red Hat Open LDAP, and Centos Open LDAP, Databases, Google apps, and other ID stores • Step up authentication • Keep the Identity in the confines of enterprise • Easy integration point for SaaS, Web and traditional applications • Easily branded and customized • Self Service User self-enrollment and identity lifecycle • Simple to use, powerful workflow • End users can securely reset their passwords and unlock their accounts (User empowerment) • Track all password activity supporting audit, compliance, and reporting • Maintain stronger password policies • Lower your Help Desk workload and reduce operating expenses • Avoid risks associated with promulgating passwords • Provide non-repudiation for high value transactions	• Flexible policy based challenge/response mechanism • User Self Service Password reset • Self Service user registration and account management • Policy based workflows • Users can lock and unlock their account for additional security (vacations, high value accounts, infrequently used accounts) • Password expiry notification • Two factor authentication for step up authentication and authorization • Webservice interfaces and REST APIs for integration with a variety of applications • Audit and usage Reports • Endpoint enforcement • Support multiple tenants from within a single instance • Flexible deployment options