DATA SHEET

CA Single Sign-On

At A Glance

CA Single Sign-On (CA SSO) provides secure and flexible access management for applications, regardless of where they're hosted or how they're accessed. Highly scalable and proven in mission-critical deployments, CA SSO enhances security by identifying who the user is and what they're attempting to do, and enforcing appropriate access policies using a standards-based framework that can be shared by IT and application developers.

KEY BENEFITS

- **Improves digital experience.** Increases user satisfaction and productivity with frictionless cross-application access.
- **Drives operational efficiencies.** Delivers centralized access management and auditing across multiple apps, devices and channels.
- **Facilitates secure DevOps.** Accelerates innovation by enabling secure access to cloud, mobile and Web apps.

KEY FEATURES

- **Secure single sign-on** provides seamless access across multiple cloud, mobile and Web applications from any device.
- **Identity federation** facilitates access to cloud, internal or partner apps via open standards, including OpenID Connect, OAuth, SAML, and WS-Federation.
- **Social login** supports dozens of identity providers, allowing your customers to leverage their social identities to log in.
- **Step-up authentication** through OpenID Connect (OIDC) lets you be more responsive to authentication requests that may require additional security, before issuing an OIDC token.
- **JSON Web token** transforms existing session tokens and shares with other authorization providers for a seamless login experience.
- **Flexible architecture models** support a variety of architecture and integration options to adapt to any environment and use case.

Business Challenges

On-premises, partner and SaaS applications are critical for supporting the transactions that drive digital business. It's essential to secure access to these applications while making it easy for consumers to quickly roll out new functionality and applications and providing a superior digital experience across all channels. However, the common challenges business face in doing so span:

User experience. Organizations are replacing or supplementing passwords with a variety of authentication mechanisms, which can be frustrating for users who want a seamless and frictionless login experience. Organizations need a security tool that supports the right credential at the right time.

Open enterprise. In today's world, applications can reside on premises or externally in the cloud. Organizations need a consistent and centralized security tool that manages access to all these apps.

Comprehensive access management. Organizations need a comprehensive access management solution that can provide omni-channel access and track activity across all channels.

Security costs. IT organizations are under constant pressure to reduce the cost of security. Consumers and employees have different access management needs, but maintaining multiple solutions for each results in unnecessary costs.

Solution Overview

CA SSO provides secure single sign-on and flexible access management to applications on premises, in the cloud and from a mobile device or a partner's site. Recognized worldwide as an industry-leading solution, CA SSO:

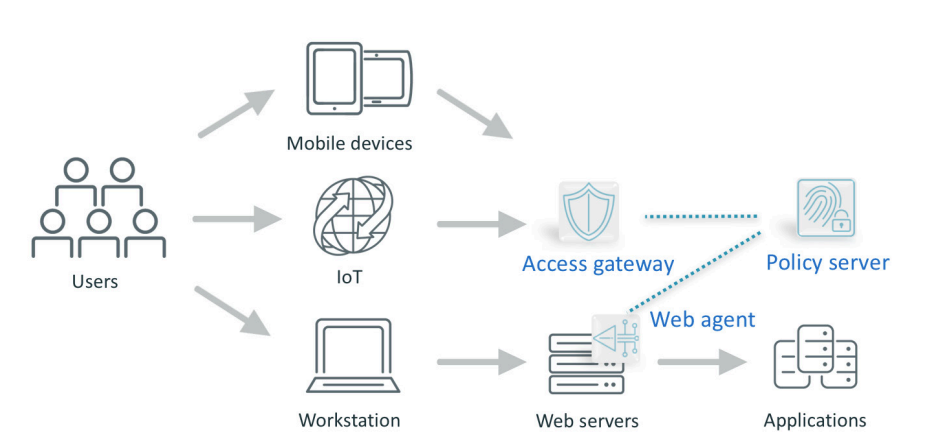
- **Delivers modern access management** and accelerates application availability by offering an unparalleled range of options for managing applications access.
- **Enhances security** by providing a common policy access layer.
- **Reduces cost of ownership** by supporting traditional Web applications, identity federation standards and Web services, all from a single, integrated high-performance platform.

Critical Differentiators

CA SSO delivers unparalleled availability, scalability and manageability. For more than two decades, CA SSO has been a leader in enterprise-class access management, providing a comprehensive solution that centrally manages access to applications and cloud services. Additional differentiators include:

- **Flexible architecture.** Supports five different SSO architectures that can be used jointly or independently to meet various business needs. The architectures are agent- and gateway-based policy enforcement points, open federation standards, formattable cookie, and REST and SOAP-based Web services.
- **Enhanced session assurance.** Impedes hackers from hijacking legitimate sessions with stolen cookies through the patented DeviceDNA™ device validation process.
- **Hybrid cloud.** Integrates with CA Identity Service to enable seamless access across cloud and on-premises applications, optionally launched via a simple-to-use integrated UI.
- **Interoperability.** Provides validated integration and SSO across hundreds of applications on a broad range of platforms, including app servers, collaboration environments, cloud apps and ERP apps.

The CA SSO environment.



Related Products

- **CA Advanced Authentication.** Identify users with two-factor credentials and risk-based authentication.
- **CA API security solutions.** Provide a trusted API security solution for integrating across apps, devices and businesses.
- **CA Directory.** Meet demanding application needs with highly reliable and scalable directory services.
- **CA Identity Service.** Accelerate and secure cloud adoption across your hybrid enterprise.

For more information, please visit **ca.com/single-sign-on**

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit ca.com/customer-success. For more information about CA Technologies, go to **ca.com.**

200-356050_0418