Upgrading CA Single Sign-On

The CA Single Sign-On (CA SSO; formerly CA SiteMinder) solution provides secure single sign-on and flexible access management to resources and applications either on-premises, in the cloud, from a mobile device or at a partner's site. Over recent releases, CA Technologies has enhanced the product to enable secure business through the support of new applications and use cases in a single platform.

The table below provides a simplified summary of enhancements introduced in recent versions. Upgrading to the latest version provides the greatest breadth of capabilities to securely enable your business. For additional detail related to the items in the table below, please review the technical guides.

Overall upgrade benefits include:

- Improved security
- Improved user experience
- Simplified administration
- Lower total cost of ownership

For additional detail related to the items in the table below, please consult the technical guides.

Features—Authentication, Authorization and Session Management	12.5*	12.51*	12.52*	12.6
Ajax support enables CA SSO to provide authentication and authorization decisions to dynamic Ajax-based applications.	✓	✓	✓	✓
Risk-based authorization improves the ability for CA SSO to make authorization decisions throughout a user's session based on the results of a risk analysis.	✓	✓	✓	✓
Expanded HTTP method support expands CA SSO's ability to provide authorization control for applications.	✓	✓	✓	✓
CA Directory support improves integration between CA SSO and CA Directory, and provides free-to-use license for CA Directory to act as key, policy and session store.	✓	✓	✓	✓
CA Identity Manager access roles enables CA Identity Suite roles to be used in CA SSO security policies, which provides tighter integration between the two products as well as improved access control.	✓	✓	✓	✓
Improved integration with Microsoft® Active Directory® enhances password services to recognize the error codes that Active Directory sends when a password cannot be reused so that CA SSO can return the password reuse message to the end user.	✓	✓	✓	✓
Open format cookies enables users to integrate homegrown applications into the CA SSO environment through the use of a lightweight, custom-built session cookie.	X	✓	✓	✓
Web services interface provides RESTful interface that applications can use to request authentication and authorization services from CA SSO.	X	✓	✓	✓

** some of these enhancements introduced in SPs and CRs on these releases*

CHART KEY:

Expanding support for enabling secure business through new applications and new use cases

Simplifying use and lowering TCO

Features—Authentication, Authorization and Session Management (continued)

Re-authentication requirement allows administrators to require users to re-authenticate every time they attempt to access a specific resource.	X	✓	✓	✓
Enhance session assurance prevents unauthorized users from hijacking legitimate sessions by stealing session cookie using a patent-pending device fingerprinting approach.	X	X	✓	✓
Expanded X.509 support allows you to link the presence of an X.509 key to a user session.	X	X	✓	✓
Improved CA Directory integration enhances password services to recognize the error codes that CA Directory returns when a password cannot be validated, so that CA SSO can return the password reuse message to the end user.	X	X	✓	✓
Session assurance improvement allows enforcement of session assurance even if the website is configured for post preservation.	X	X	X	✓
Authentication, Authorization and Session Management—Federation	**12.5***	**12.51***	**12.52***	**12.6**
CA Directory support allows attributes from SAML assertions or OAuth tokens to be maintained for use in authorization decisions when CA Directory is used as session store in federation use cases.	✓	✓	✓	✓
Authentication context support provides the ability for a service provider (SP) to enforce a stronger form of user authentication before providing access to a resource.	✓	✓	✓	✓
User consent enforcement allows user consent to be required before any identity information is sent from the identity provider (IdP) to the SP. This can be set by CA SSO when acting as either IdP or SP.	✓	✓	✓	✓
Attribute mapping enables an SP to support multiple IdPs for a single application by mapping user attributes differently for each IdP.	✓	✓	✓	✓
Dynamic user provisioning provides an interface to configure just-in-time provisioning to support new users who need access to SP applications.	✓	✓	✓	✓
Expanded single logoff (SLO) enables the use of CA SSO for federated SLO with more applications.	✓	✓	✓	✓
Expanded Java™ and .Net SDK broadens the application integration capabilities of CA SSO for Open Format Cookies and federation transactions.	✓	✓	✓	✓
OAuth Relying Party (RP) support provides the ability to configure CA SSO to validate OAuth tokens provided by Google and Facebook.	X	✓	✓	✓
Browser-based SSO to Office 365® offers support for browser-based access via the WS-Federation protocol.	X	✓	✓	✓
SAML attribute query enables CA SSO to query IdP for more information when the initial assertion does not include all the necessary attributes to successfully complete the federated single sign-on transaction.	X	✓	✓	✓
Attribute transformation enables CA SSO to manipulate or customize user attributes when generating an assertion or claim, which helps to improve user experience and simplify integration between partners.	X	✓	✓	✓

** some of these enhancements introduced in SPs and CRs on these releases*

CHART KEY:

Expanding support for enabling secure business through new applications and new use cases

Simplifying use and lowering TCO

Authentication, Authorization and Session Management— Federation (continued)

Attribute persistence allows CA SSO to maintain user attributes from SAML assertions or OAuth tokens in the session store, so that they can be used for authorization decisions throughout the user's session.	X	✓	✓	✓
Expanded OAuth RP support expands the ability to configure CA SSO to validate OAuth tokens provided by LinkedIn, Microsoft Live and Twitter.	X	X	✓	✓
Enhanced NameID support enables the de-provisioning of an individual user from a partnership.	X	X	✓	✓
Thick client-based SSO to Office 365 expands single sign-on support for Microsoft Office 365 to support thick clients such as Excel®, Word and PowerPoint® using the WS-Federation active profile protocol.	X	X	✓	✓
SAML 2.0 post binding supported as a method for exchanging requests and responses during authentication and single log-out requests.	X	X	✓	✓
Failed authentication notification support allows an administrator to configure a notification to the SP when a user fails authentication, so that the SP can determine the appropriate action to take.	X	X	✓	✓
Enhanced social sign-on enables users to access a federated resource using their social networking credentials instead of the federation system credentials.	X	X	✓	✓
IWA-based SSO to Microsoft Office 365 enables IWA authentication and single sign-to Microsoft Office 365 via thick clients.	X	X	✓	✓
Dynamic authentication enables single federation partnership to support multiple forms of authentication based on sensitivity of the application on SP side.	X	X	X	✓
Attribute consuming service (ACS) enhancements supports ACS Index and ACS URL in authentication request.	X	X	X	✓
Enhanced certificate support supports secondary certificates and certificate expiration details in federation partnerships and the ability to update certificates without deactivating the partnership.	X	X	X	✓
Component: CA Access Gateway (formerly CA SiteMinder Secure Proxy Server or SPS)	**12.5***	**12.51***	**12.52***	**12.6**
WebDav support enables CA SSO to extend authentication and authorization to additional classes of applications using this protocol.	✓	✓	✓	✓
Incorporated session linker enables CA SSO session to be linked to session tokens for applications being protected by CA SSO, such as IBM®WebSphere® and SAP. This improves security by protecting these tokens from being hijacked.	✓	✓	✓	✓
Application server agent (ASA) support enables you to use ASAs with the gateway instead of a Web agent, allowing you to reduce the complexity and TCO of your CA SSO infrastructure.	✓	✓	✓	✓
IWA support enables you to remove other CA SSO IIS Web agents that may only have been being used to provide the IWA support in your SSO infrastructure.	✓	✓	✓	✓
Enhanced proxy rules provide the ability to support more access management use cases.	✓	✓	✓	✓

** some of these enhancements introduced in SPs and CRs on these releases*

CHART KEY:

Expanding support for enabling secure business through new applications and new use cases

Simplifying use and lowering TCO

Administration and Supportability (continued)

Administration and Supportability	12.5*	12.51*	12.52*	12.6
Hardware load balancer support between agents and policy servers to allow multiple policy servers to be exposed to agents through one or more virtual IP addresses	✓	✓	✓	✓
Key store consolidation allows keys to be moved into the policy store, which replaces the need for multiple, local smkey databases with a single certificate data store.	✓	✓	✓	✓
Enhanced directory mapping simplifies the ability to employ user information from the repository where it already exists, thereby reducing the need for significant user repository re-architecture.	✓	✓	✓	✓
Enhanced Admin UI security allows the Admin UI to be protected by CA SSO authentication.	✓	✓	✓	✓
Agent discovery allows you to view agent-specific details such as version, state of operation and agent configuration objects within the Admin UI. You can also view a list of agents deployed on various hosts in your enterprise and delete the unwanted agent instance entries from the list.	✓	✓	✓	✓
Administration workspaces enables fine-grained delegation of CA SSO tasks, which define their administrative authority.	✓	✓	✓	✓
Integrated advanced password services provide a comprehensive set of password-management capabilities that extend beyond what basic password services provides.	✓	✓	✓	✓
Federation partnership management was enhanced with a wizard-driven approach for creating, updating, suspending and deleting federation partnerships. The federation UI was also consolidated with Admin UI to provide a single interface for managing the entire CA SSO environment.	✓	✓	✓	✓
Federation administrative scoping provides additional flexibility and fine-grained access control over privileges to manage federated partnerships.	✓	✓	✓	✓
Expanded performance management support enables integration with CA Application Performance Management (CA APM) with the CA Access Gateway to allow you to monitor the performance of the embedded gateway Web agent.	✓	✓	✓	✓
Expanded agent discovery supported improves the visibility into the number and configuration of CA Access Gateway instances in the CA SSO environment.	✓	✓	✓	✓
Administrative UI for CA Access Gateway simplifies the configuration and management of the access gateways.	✓	✓	✓	✓
Multiple access gateway instance support allows you to host multiple instances of the gateway on the same server via group configuration.	✓	✓	✓	✓
Enhanced search enables administrators to search for resources, roles and responses.	X	✓	✓	✓
Attribute management provides the ability to select attributes from session store for inclusion in a SAML assertion or HTTP responses.	X	✓	✓	✓
Assertion attribute logging allows administrators to record any assertion attributes used in transactions to the policy server logs.	X	✓	✓	✓

** some of these enhancements introduced in SPs and CRs on these releases*

CHART KEY:

Expanding support for enabling secure business through new applications and new use cases

Simplifying use and lowering TCO

Administration and Supportability (continued)

Assertion attribute logging allows administrators to record any assertion attributes used in transactions to the policy server logs.	X	✓	✓	✓
Enhanced user disambiguation improves and simplifies the use of the Kerberos and IWA authentication schemes.	X	X	✓	✓
Detailed federation transaction logging enables improved troubleshooting support. If a federation transaction fails, the checkpoint messages and transaction IDs can help you determine the specific problem.	X	X	✓	✓
Just-in-time provisioning interface for OAuth identities enables organizations to more quickly support new users needing access to RP-side applications.	X	X	✓	✓
Federation certificate management provides certificate list that cross-references partnerships.	X	X	✓	✓
Enhanced Admin UI enables improved sorting and searching in the domain policies page of the administrative user interface.	X	X	✓	✓
Packaged CA remote engineer delivered by CA SSO greatly simplifies the ability to collect and securely deliver environmental and audit log data to CA Support, helping to accelerate troubleshooting and problem resolution.	X	X	✓	✓
Embedded policy object repair simplifies the identification and cleanup of invalid policy objects, ensuring simpler upgrade and reliability.	X	X	✓	✓
Enhanced algorithm for trace log capture improves the performance and reliability for gathering detailed tracing data when troubleshooting a service problem.	X	X	✓	✓
Multiple ACO support for IIS Web agent allows admins to use different setting for each IIS website when they are using shared IIS servers.	X	X	✓	✓
Turn off authorization calls for Web agents allows organizations that are only using agents for authentication to turn off authorization calls, which produces faster response times and reduced network traffic.	X	X	✓	✓
ACO searching allows admins to search for ACOs in the Admin UI.	X	X	X	✓
Platforms and Internals	**12.5***	**12.51***	**12.52***	**12.6**
Operating system support for the server components:				
Red Hat 6	✓	✓	✓	✓
Red Hat 7	X	X	X	✓
Standardized internationalization and localization extended to additional languages: French, German, Italian, Spanish, Korean and Brazilian Portuguese (in addition to the longstanding Japanese translation).	X	✓	✓	✓
Syslog support allows administrators to direct policy server audit data to the syslog on supported UNIX® operating environments.	X	✓	✓	✓

** some of these enhancements introduced in SPs and CRs on these releases*

CHART KEY:

Expanding support for enabling secure business through new applications and new use cases

Simplifying use and lowering TCO

Performance improvements specifically focused on administration of large policy stores and session store.	X	X	✓	✓
64-bit support allows all server components to be run as 64-bit applications.	X	X	X	✓
SSL accelerator support allows CA Access Gateway to support environments where outward-facing load balancers support SSL acceleration.	X	X	X	✓
Safari browser support expands Microsoft Office 365 single sign-on support to Safari browsers.	X	X	X	✓
Simplified session assurance installation removes dependence on CA Risk Authentication server component to support enhanced session assurance.	X	X	X	✓
Performance improvements remove performance bottlenecks and enable organizations to support more access control with fewer system resources providing ROI improvements.	*At each release*			
Licensing	**12.5***	**12.51***	**12.52***	**12.6**
Free use of CA Directory enables organization to use CA Directory free of charge as a policy store, session store or key store. Paid licenses are still required if you want to use CA Directory as a user store.	✓	✓	✓	✓
Free use of CA Access Gateway (formerly CA SiteMinder Secure Proxy Server or SPS). The CA Access Gateway license has been incorporated into the base CA SSO license.[1]	X	✓	✓	✓
Free unlimited federation partnerships are included for all licensed CA SSO users for any customer who has purchased or upgrade to CA SSO r12.51 or higher.	X	✓	✓	✓

** some of these enhancements introduced in SPs and CRs on these releases*

CHART KEY:

Expanding support for enabling secure business through new applications and new use cases

Simplifying use and lowering TCO

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

1 The CA Access Gateway is provided free of charge as part of the CA SSO license to all new customers who purchase CA SSO r12.51 or higher. For existing customers that have owned CA SSO prior to the GA of 12.51, the CA Access Gateway can be used free of charge if the customer never purchased the CA Secure Proxy Server (SPS) and upgrades to the r12.51 or higher.

CS200-233422_1116