Why Upgrade to CA Single Sign-On 12.7

CA Single Sign-On (CA SSO) provides secure and flexible web single sign-on and access management for your applications—regardless of where they're hosted or how they're accessed. CA SSO is highly scalable and enhances security by identifying who the user is, what they're attempting to do and enforcing appropriate access policies using standards-based frameworks that can be shared by IT and application developers.

Upgrading to the latest CA SSO version provides new features, cumulative bug fixes, performance improvements and a longer support lifecycle. Key enhancements available in CA SSO 12.7 include:

1. **OpenID Connect support.** Secure your web apps with the OpenID Connect authorization code flow, which uses compact JSON tokens to exchange data instead of XML-based SAML tokens.
2. **REST APIs for administration.** Create and modify federation partnerships and security policies from your own administration user interfaces via REST-based web services calls.
3. **Integrated Windows Authentication (IWA) fallback.** Support multiple secondary authentication fallback options through chaining when primary IWA fails.
4. **Remote Engineer 4.0 with telemetry.** Reduce support troubleshooting and resolution time via a service that communicates your configuration details to CA Support.
5. **Platform modernization.** Provide support for 64-bit policy server.

For additional detail related to the items in the table below, please review the product documentation.

Authentication, Authorization and Session Management

The table below provides a simplified summary of enhancements to the authentication, authorization and session management capabilities that were introduced in recent versions.

Enhancements to Authentication, Authorization and Session Management	12.52*	12.6*	12.7
Session assurance prevents unauthorized users from hijacking legitimate sessions by stealing session cookie using a patent-pending, device-fingerprinting approach.	✓	✓	✓
Expanded X.509 support allows you to link the presence of a X.509 key to a user session.	✓	✓	✓
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.	✓	✓	✓
Session assurance improvement allows enforcement of session assurance even if the website is configured for post preservation.	X	✓	✓
IWA fallback enhancement allows the fallback process to combine multiple secondary authentication schemes as a new authentication chain if the primary IWA fails.	X	X	✓
SecurID HTML form template enhancement improves the user experience by not prompting the user to re-enter the username and passcode once the user authentication succeeds in the login page.	X	X	✓

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

Identity Federation

The table below provides a simplified summary of enhancements to the identity federation capabilities that were introduced in recent versions.

Features: Identity Federation	12.52*	12.6*	12.7*
Expanded OAuth RP support expanded the ability to configure CA SSO to validate OAuth tokens provided by Google, Facebook, LinkedIn, Microsoft Live and Twitter.	✓	✓	✓
Enhanced NameID support enables the deprovisioning of an individual user from a partnership.	✓	✓	✓
Thick-client-based SSO to Microsoft Office 365® expands single sign-on support for Office 365 to support thick clients such as Excel®, Word and PowerPoint® using the WS-Federation active profile protocol.	✓	✓	✓
SAML 2.0 post binding supported as a method for exchanging requests and responses during authentication and single logout requests.	✓	✓	✓
Failed authentication notification support allows an administrator to configure a notification to the SP when a user fails to authenticate so that the SP can determine the appropriate action to take.	✓	✓	✓
IWA-based SSO to Office 365 enables IWA authentication and single sign-on to Office 365 via thick clients.	✓	✓	✓
CA Identity Service integration allows CA SSO to act as IDP for users logging into the cloud service.	✓	✓	✓
Dynamic authentication enables single federation partnership to support multiple forms of authentication based on sensitivity of the application on SP side.	X	✓	✓
Attribute Consuming Service (ACO) enhancements supports ACS Index and ACS URL in authentication request.	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	✓	✓
XPSConfig utility enhancement introduces a new parameter, AllowNativeDisabledUserCheck. By changing the value of this parameter to TRUE, you can deny access to the native disabled users at SP side user directory.	X	X	✓
OpenID Connect allows CA SSO to act as an OIDC provider using the OpenID Connect 1.0 protocol. The protocol allows clients to verify the identity of the users that are authenticated by the authorization server, and obtain basic profile information.	X	X	✓

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

Administration and Supportability

The table below provides a simplified summary of enhancements to the administration and supportability capabilities that were introduced in recent versions.

Enhancements to Administration and Supportability	12.52*	12.6*	12.7
Enhanced user disambiguation improves and simplifies the use of the Kerberos and IWA authentication schemes.	✓	✓	✓
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.	✓	✓	✓
Just-in-time provisioning interface for OAuth identities enables organizations to more quickly support new users needing access to RP-side applications.	✓	✓	✓
Federation certificate management provides certificate list that cross-references partnerships.	✓	✓	✓
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.	✓	✓	✓
Multiple ACO support for IIS web agent allows admins to use different settings for each IIS website when they are using shared IIS servers.	✓	✓	✓
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.	✓	✓	✓
ACO searching allows admins to search for ACOs in the Admin UI	✓	✓	✓
Updated CA Remote Engineer 4.0 added to the solution.	X	✓	✓
Management REST APIs provides the following new Policy Object REST APIs: ▪ Administrative token API—Obtain a JWT token that is required to access the Policy Data API. ▪ Policy data API—Create, read, update and delete objects (including federation entities and partnerships and certificate services) in the policy store. ▪ Policy import/export API—Export and import specified subsets of the policy data in the policy store.	X	X	✓
Administrative UI cache maintains a cache for managing certificates to avoid a number of calls between policy server and admin UI. A new option, Get Updates, is introduced to synchronize the certificates information in administrative UI with the changes available in the certificate store.	X	X	✓
OpenID Connect administration creates a new security category OpenID Connect administration in the admin UI that allows you to set privileges and rights of an administrator for managing the OpenID Connect feature.	X	X	✓

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

Enhancements to Administration and Supportability	12.52*	12.6*	12.7
View object dependencies allows you to view the list of objects that depend on a specific object in CA SSO (e.g., you can view the list of partnerships that are using a certificate).	X	X	✓
Configuring GUID Cookie Validity Duration allows you to manage the AuthnRequest state when the AuthnRequest binding is configured to HTTP-POST by adding the GUID Cookie Validity Duration (Seconds) parameter in the administrative UI.	X	X	✓
Name qualifier query parameter is now supported in the AuthnRequest	X	X	✓
Enhanced web application client response allows configuration of the response format for requests from Web 2.0 resources at a global level. This option reduces the need to manually configure requests/responses at each web agent.	X	X	✓
**Some of these enhancements introduced in SPs and CRs on these releases.*			

Platform Support and Internals

The table below provides a simplified summary of new platform certifications for the server components and enhancements to the solution internals that were introduced in recent versions.

Enhancements to Platform Support and Internals	12.52*	12.6*	12.7
Performance improvements removes performance bottlenecks and enables organizations to support more access control with fewer system resources, providing ROI improvements.	✓	✓	✓
64-bit support—all server components can now be run as 64-bit applications.	X	✓	✓
SSL accelerator support—CA Access Gateway can now support environments where outward-facing load balancers support SSL acceleration.	X	✓	✓
Safari browser support expands Office 365 single sign-on support to Safari browsers.	X	✓	✓
Simplified session assurance installation removes dependence on the CA Risk Authentication server component to support enhanced session assurance.	X	✓	✓
Web Agent Support for dynamically scaled environments allow SSO Web Agents to be used in dynamically scaled environments such as Docker containers and OpenShift.	X	X	✓
**Some of these enhancements introduced in SPs and CRs on these releases.*			

To learn more about CA Single Sign-On, visit ca.com/single-sign-on

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**.

CS200-274492_0518