Why Upgrade to CA Single Sign-On 12.8

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 and what they're attempting to do, and by enforcing appropriate access policies using standards–based frameworks that can be shared by IT and application developers.

Upgrading to the latest version of CA Single Sign-On provides the best value for your investment, as it provides the latest features, new certifications, cumulative bug-fixes and a longer support lifecycle.

Key new features and enhancements in CA SSO 12.8 include:

1) **JSON Web Token (JWT) authentication scheme,** which enables CA SSO to accept compact JWTs for authentication.
   - ✓ Enables CA SSO to act as an OpenID Connect Resource Server and validate a JWT generated from an external OpenID Connect Provider
   - ✓ Provides enhanced integration with CA API Management and other API management solutions that can generate JWTs
   - ✓ Supports claims-based authorization for access to protected resources using the claims in the JWT
2) **Many OpenID Connect enhancements,** including these highlights:
   - ✓ Refresh token support improves user experience by renewing the access token upon expiration without requiring the end user to reauthenticate
   - ✓ Implicit flow support enables use of CA SSO as OpenID Connect Provider for client-side script applications, such as single-page applications, running in the Web browser
   - ✓ Proof Key for Code Exchange (PKCE) and step-up authentication options enhance security of the flows
3) **JSON request and response** support is added to the REST APIs for authentication and authorization Web services available via the CA Access Gateway.
4) **IP whitelisting** in the authentication scheme configuration to control which agents can execute specific trust-based authentication schemes, such as X.509 or Microsoft Windows®.
5) The policy server, administration UI, access gateway and SDK supported on **Microsoft Windows Server 2016®,** in addition to Microsoft Windows Server 2012 R2.

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	12.8
Session assurance prevents unauthorized users from hijacking legitimate sessions by stealing session cookies, using a patent–pending, device–fingerprinting approach.	✓	✓	✓	✓
Session assurance allows enforcement of session assurance for websites configured for post-preservation.	X	✓	✓	✓
Integrated Windows Authentication (IWA) fallback enhancement allows the Microsoft Windows authentication with fall back to forms if the primary IWA fails.	X	X	✓	✓
SecurID HTML 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	✓	✓
IP whitelisting in the authentication scheme restricts access by validating agent IPs against a set of restricted IPs.	X	X	X	✓
JSON Web Token (JWT) authentication scheme enables CA SSO to accept compact JWTs for authentication.	X	X	X	✓
CA SSO serves as OpenID Connect (OIDC) Resource Server by accepting the JWT generated by any OIDC provider, including an enhanced integration with CA API Management. (Note: CA SSO is not an OIDC relying party.)	X	X	X	✓
JSON request and response for CA SSO authentication and authorization **REST API.**	X	X	X	✓
Step-up authentication using authentication context prior to issuing an OIDC token.	X	X	X	✓

**Some of these enhancements were 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	12.8
Expanded OAuth RP support expands the ability to configure CA SSO to validate OAuth tokens provided by Google, Facebook, LinkedIn, Microsoft Live and Twitter.	✓	✓	✓	✓
SAML 2.0 post binding supported as a method for exchanging requests and responses during authentication and single logout requests.	✓	✓	✓	✓
IWA–based SSO to Office 365 enables IWA authentication and single sign-on to Microsoft Office 365 via thick clients.	✓	✓	✓	✓
CA Identity Service integration provides a unified launchpad for applications served out of CA Identity Service and CA SSO.	✓	✓	✓	✓
Dynamic authentication enables single federation partnership to support multiple forms of authentication based on sensitivity of the application on service provider side..	X	✓	✓	✓

**Some of these enhancements were introduced in SPs and CRs on these releases.*

Features: Identity Federation	12.52*	12.6*	12.7	12.8
SAML 2.0 service provider supports Attribute Consuming Service Index and Assertion Consumer Service URL in authentication request to the provider.	X	✓	✓	✓
Enhanced certificate support. Parallel secondary signing certificates, certificate expiration details visible in federation partnership configuration UI, and the ability to update certificates without deactivating the partnership.	X	✓	✓	✓
SAML service provider integration with native user store account settings that allows you to deny access to users that are disabled in user repositories on the service provider side.	X	X	✓	✓
OpenID Connect authorization code flow 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	✓	✓
OpenID Connect implicit flow enables CA SSO to act as OIDC provider to client-side script applications (e.g., single page apps) running in the Web browser.	X	X	X	✓
OpenID Connect refresh token support generates a renewed access token upon expiry.	X	X	X	✓
PKCE and step-up authentication support offer greater security in OpenID Connect flows.	X	X	X	✓
OpenID Connect introspection endpoint validates the access or refresh token and gives the response with the token details along with the scope.	X	X	X	✓
Custom URI as the Redirect URI in OIDC flow.	X	X	X	✓

**Some of these enhancements were introduced in SPs and CRs on these releases.*

Administration, Internals 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	12.8
Web agent support for dynamically scaled environments allows CA SSO Web agents to be used in dynamically scaled environments such as Docker containers and OpenShift.	✓	✓	✓	✓
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.	✓	✓	✓	✓
SSL accelerator support—CA Access Gateway can now support environments where outward-facing load balancers support SSL acceleration.	X	✓	✓	✓
Safari browser support expands Microsoft Office 365 single sign-on support to Safari browsers.	X	✓	✓	✓
Management REST APIs provide 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	✓	✓

**Some of these enhancements were introduced in SPs and CRs on these releases.*

Enhancements to Administration and Supportability	12.52*	12.6*	12.7	12.8
Simplified session assurance installation removes dependence on the CA Risk Authentication server component to support enhanced session assurance.	X	✓	✓	✓
Management REST APIs provide the following new policy object REST APIs: • Administrative token API—Obtain a JWT 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—Certificates are now cached in the UI to increase UI performance.	X	X	✓	✓
OpenID Connect administration creates a new security category in the admin UI that allows you to set privileges and rights of an administrator for managing the OpenID Connect feature.	X	X	✓	✓
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 Globally Unique Identifier (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 were introduced in SPs and CRs on these releases.*

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

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**.

200-350093_0418