CA Single Sign-On - 12.7

Release Comparison

Date: 10-May-2017

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2017 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Release Comparison

This table compares the key features in all active releases for CA Single Sign-On. Upgrading to latest releases provides:

- New features
- Improved User Experience
- Cumulative bug fixes
- Longer support life cycle

Note: * some of these enhancements were introduced in service packs and cumulative releases over these releases.

Features—Authentication, Authorization, and Session Management	12.51*	12.52*	12.6*	12.7
Policy Object REST APIs (https://docops.ca.com/display/casso127/Policy+Object+REST+APIs) allow you to create, read, update, and delete objects in the policy store and export and import specified subsets of the policy data in the policy store.	No	No	No	Yes
Authentication Chaining (https://docops.ca.com/display/casso127/Authentication+Chaining) allows Integrated Windows Authentication (IWA) to fallback to a forms-based authentication scheme.	No	No	No	Yes
Support for 64-bit Policy Server (https://docops.ca.com/display/casso127/Policy+Server+Installation+Requirements).	No	No	Yes	Yes
Session assurance (https://docops.ca.com/pages/viewpage.action?pageId=373941050) improvement allows enforcement of session assurance even if the website is configured for post preservation.	No	No	Yes	Yes
Enhanced session assurance (https://docops.ca.com/pages/viewpage.action?pageId=373941032) prevents unauthorized users from hijacking legitimate sessions by stealing session cookie using a patent-pending device fingerprinting approach.	No	Yes	Yes	Yes
Expanded X.509 support (https://docops.ca.com/display/casso127/X.509+Client+Certificate+Authentication+Schemes) allows you to link the presence of an X.509 key to a user session.	No	Yes	Yes	Yes
Improved CA Directory integration **enhances password services** (https://docops.ca.com/display/casso127/How+to+Configure+Password+Policies) 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.	No	Yes	Yes	Yes
Ajax support (https://docops.ca.com/pages/viewpage.action?pageId=373941050) enables CA SSO to provide authentication and authorization decisions to dynamic Ajax-based applications.	Yes	Yes	Yes	Yes
Risk-based authorization (https://docops.ca.com/display/casso127/Integration+with+CA+Strong+Authentication+and+CA+Risk+Authentication) improves the ability for CA SSO to make authorization decisions throughout a user's session based on the results of a risk analysis.	Yes	Yes	Yes	Yes
CA Identity Manager access roles (https://docops.ca.com/display/casso127/CA+Identity+Manager+Roles+and+Access+Control) enables CA Identity Suite roles to be used in CA SSO security policies, which provide tighter integration between the two products (https://docops.ca.com/display/casso127/Integration+with+CA+Identity+Manager) and improved access control.	Yes	Yes	Yes	Yes
Open format cookies (https://docops.ca.com/display/casso127/Open+Format+Cookie+Details) enables users to integrate homegrown applications into the CA SSO environment by using a lightweight, custom-built session cookie.	Yes	Yes	Yes	Yes
Web services interface (https://docops.ca.com/display/casso127/Configuring+the+Authentication+and+Authorization+Web+Services) provides RESTful and SOAP web interfaces that applications can use to request authentication and authorization services from CA SSO.	Yes	Yes	Yes	Yes
	Yes	Yes	Yes	Yes

Features—Authentication, Authorization, and Session Management	12.51*	12.52*	12.6*	12.7
Re-authentication requirement (https://docops.ca.com/display/casso127/How+to+Require+Re-authentication+for+Sensitive+Resources) allows administrators to require users to re-authenticate every time they attempt to access a specific resource.				

Features— Federation	12.51*	12.52*	12.6*	12.7
CA Single Sign-On authenticates users using OpenID Connect- Authorization Code Flow that uses code as the response type. For more information, see Use CA Single Sign-On as OpenID Connect Provider. (https://docops.ca.com/display/casso127/Use+CA+Single+Sign-On+as+OpenID+Connect+Provider)	No	No	No	Yes
AllowNativeDisabledUserCheck parameter in the XPSConfig utility allows you to deny access to the native disabled users at SP side user directory for certain directories. See **User Identification for a Partnership** (https://docops.ca.com/display/SITEMINDER/.User+Identification+for+a+Partnership+v12.7) and Authentication Schemes (https://docops.ca.com/display/SITEMINDER/.Authentication+Schemes+v12.7) .	No	No	No	Yes
GUID Cookie Validity Duration (Seconds) parameter in the Administrative UI to manage the AuthnRequest state when the AuthnRequest binding is configured to HTTP-POST, theI. See SSO and SLO Dialog (SAML 2.0 IdP) (https://docops.ca.com/display/SITEMINDER/.SSO+and+SLO+Dialog+%28SAML+2.0+IdP%29+v12.7) .	No	No	No	Yes
Dynamic authentication (https://docops.ca.com/pages/viewpage.action?pageId=373941304) enables single federation partnership to support multiple forms of authentication based on sensitivity of the application on SP side.	No	No	Yes	Yes
Attribute consuming service (https://docops.ca.com/display/casso127/URLs+to+Initiate+Single+Sign-on) (ACS) enhancement supports ACS Index and ACS URL in authentication request.	No	No	Yes	Yes
Enhanced certificate supports (https://docops.ca.com/display/casso127/Signature+and+Encryption+Configuration+for+Federated+Partnerships) secondary certificates and certificate expiration details in federation partnerships and the ability to update certificates without deactivating the partnership.	No	No	Yes	Yes
Expanded OAuth RP support expands the ability to configure CA SSO to validate OAuth tokens provided by LinkedIn, Microsoft Live and Twitter (https://docops.ca.com/display/casso127/Configure+Social+Sign-on).	No	Yes	Yes	Yes
OAuth Relying Party (RP) support provides the ability to configure CA SSO to validate OAuth tokens provided by Google and Facebook (https://docops.ca.com/display/casso127/Configure+Social+Sign-on).	Yes	Yes	Yes	Yes
Enhanced NameID (https://docops.ca.com/pages/viewpage.action?pageId=373941294) support enables the deprovisioning of an individual user from a partnership.	No	Yes	Yes	Yes
Thick client-based SSO to Office 365 (https://docops.ca.com/display/casso127/Single+Sign-on+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.	No	Yes	Yes	Yes
	Yes	Yes	Yes	Yes

Features— Federation	12.51*	12.52*	12.6*	12.7
Browser-based SSO to Office 365® (https://docops.ca.com/display/casso127/Single+Sign-on+to+Office+365) offers support for browser-based access via the WS-Federation protocol.				
SAML 2.0 post binding (https://docops.ca.com/display/casso127/Enable+SAML+2.0+HTTP-POST+Binding) supported as a method for exchanging requests and responses during authentication and single logout requests.	No	Yes	Yes	Yes
Failed authentication notification (https://docops.ca.com/display/casso127/SAML+2.0+Response+for+Authentication+Failure)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.	No	Yes	Yes	Yes
Integrated Windows Authentication (IWA) -based SSO to Microsoft Office 365 (https://docops.ca.com/display/casso127/Single+Sign-on+to+Office+365) enables IWA authentication and single sign-to Microsoft Office 365 using thick clients.	No	Yes	Yes	Yes
Authentication context (https://docops.ca.com/display/casso127/Enable+Authentication+Context+Requests+at+the+SP-to-IdP+Partnership) support provides the ability for a service provider (SP) to enforce a stronger form of user authentication before providing access to a resource.	Yes	Yes	Yes	Yes
User consent enforcement (https://docops.ca.com/display/casso127/User+Consent+at+a+SAML+2.0+IdP) 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.	Yes	Yes	Yes	Yes
Attribute mapping (https://docops.ca.com/display/casso127/User+Attribute+Mapping)enables an SP to support multiple IdPs for a single application by mapping user attributes differently for each IdP.	Yes	Yes	Yes	Yes
Dynamic user provisioning (https://docops.ca.com/display/casso126/User+Provisioning+at+the+Relying+Party) provides an interface to configure just-in-time provisioning to support new users who need access to SP applications.	Yes	Yes	Yes	Yes
Single logoff (SLO) (https://docops.ca.com/pages/viewpage.action?pageId=373941329) enables the use of CA SSO for federated SLO with more applications.	Yes	Yes	Yes	Yes
Java™ and .Net SDK (https://docops.ca.com/display/casso127/Open+Format+Cookie+Details) broadens the application integration capabilities of CA SSO for Open Format Cookies and federation transactions.	Yes	Yes	Yes	Yes
SAML attribute query support (https://docops.ca.com/display/casso127/SAML+2.0+Attribute+Query+Support)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.	Yes	Yes	Yes	Yes
Attribute transformation (https://docops.ca.com/display/casso127/How+to+Configure+Claims+Transformation+at+the+Asserting+Party) 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.	Yes	Yes	Yes	Yes
Attribute persistence (https://docops.ca.com/display/casso127/Federation+Features+Requiring+the+Session+Store) 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.	Yes	Yes	Yes	Yes

Component: CA Access Gateway (formerly CA SiteMinder Secure Proxy Server or SPS)	12.51 *	12.52 *	12.6 *	12.7
Session linker (https://docops.ca.com/display/casso127/Synchronize+SSO+and+Third-Party+Application+Sessions) enables CA SSO session to be linked to session tokens for applications being protected by CA SSO, such as IBM®WebSphere® and SAP. This feature improves security by protecting these tokens from being hijacked.	Yes	Yes	Yes	Yes
Application server agent (https://docops.ca.com/display/casso127/CA+Single+Sign-On+Agents+Overview)(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.	Yes	Yes	Yes	Yes
Integrated Windows Authentication (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.	Yes	Yes	Yes	Yes
Enhanced proxy rules (https://docops.ca.com/display/casso127/CA+Access+Gateway+Architecture+Introduced) provide the ability to support more access management use cases.	Yes	Yes	Yes	Yes

Administration and Supportability	12.51 *	12.52 *	12.6 *	12.7
To reduce the number of calls between the Policy Server and Administrative UI, the Administrative UI now uses a cache for certificate management. For more information, see **Trusted Certificates and Private Keys** (https://docops.ca.com/display/casso127/Trusted+Certificates+and+Private+Keys) .	No	No	No	Yes
New **OpenID Connect Administration** security category in the Administrative UI lets you set privileges and rights of an administrator for managing the OpenID Connect feature. See Select Security Category (https://docops.ca.com/display/SITEMINDER/.Select+Security+Category+Page+v12.7) .	No	No	No	Yes
CA SSO supports using Web Agents in dynamically scaled environments such as Docker containers, OpenShift. For more information, see Use Web Agent in Dynamically Scaled Environments (https://docops.ca.com/display/casso127/Use+Web+Agent+in+Dynamically+Scaled+Environments)**.**	No	No	No	Yes
Object Dependencies (https://docops.ca.com/display/casso127/Object+Dependencies) feature allows you to view the list of objects that depend on a specific object.	No	No	No	Yes
ACO parameter searching (https://docops.ca.com/display/casso127/Agent+Configuration+Dialog+Settings) allows administrators to search for specific parameters of ACOs in the Administrative UI.	No	No	Yes	Yes
Out of the box **integration with Remote Engineer and Telemetry Service** (https://docops.ca.com/ca-remote-engineer/4-0/en/integrating-with-remote-engineer/integrate-ca-remote-engineer-with-ca-telemetry-service) to verify alignment with recommended configurations and to reduce the time to triage support issues	No	No	Yes	Yes
Enhanced user disambiguation improves and simplifies the use of the Kerberos and IWA authentication schemes.	No	Yes	Yes	Yes
Detailed federation transaction logging (https://docops.ca.com/display/casso127/Log+Files+that+Aid+Partnership+Federation+Troubleshooting)enables improved troubleshooting support. If a federation transaction fails, the checkpoint messages and transaction IDs can help you determine the specific problem.	No	Yes	Yes	Yes

Administration and Supportability	12.51*	12.52*	12.6*	12.7
Just-in-time provisioning interface for OAuth identities enables organizations to more quickly support new users needing access to RP-side applications.	No	Yes	Yes	Yes
Federation certificate management (https://docops.ca.com/display/casso127/Key+and+Certificate+Management+for+Federation) provides certificate list that cross-references partnerships.	No	Yes	Yes	Yes
Enhanced algorithm for trace log capture (https://docops.ca.com/display/casso127/How+to+Set+Up+Trace+Logging) improves the performance and reliability for gathering detailed tracing data when troubleshooting a service problem.	No	Yes	Yes	Yes
Multiple Agent Configuration Objects (ACO) support (https://docops.ca.com/display/casso127/Apply+CA+Single+Sign-On+Behavior+to+a+Web+Application+Client) for IIS Web Agent allows admins to use different setting for each IIS website when they are using shared IIS servers.	No	Yes	Yes	Yes
Turn off authorization calls for Web agents (https://docops.ca.com/display/casso127/Manage+Web+Agent+Authorization) allows organizations that are only using agents for authentication to turn off authorization calls, which produce faster response times and reduced network traffic.	No	Yes	Yes	Yes
Packaged CA Remote Engineer (CARE) (https://docops.ca.com/display/casso127/Use+the+CA+Remote+Engineer+Tool+to+Collect+Troubleshooting+Data+for+CA+Support) 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.	No	Yes	Yes	Yes
Integration with CA Identity Service allows you to provide access to CA Single Sign-On apps for people in CA Identity Service. For more information, see **Integration with CA Identity Service**. (https://docops.ca.com/display/casso127/Integration+with+CA+Identity+Service)	Yes	Yes	Yes	Yes
Hardware load balancer support between agents and policy servers (https://docops.ca.com/display/casso127/Configure+Agent+to+Policy+Server+Communication+Using+a+Hardware+Load+Balancer) to allow multiple policy servers to be exposed to agents through one or more virtual IP addresses.	Yes	Yes	Yes	Yes
Directory mapping (https://docops.ca.com/display/casso127/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.	Yes	Yes	Yes	Yes
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.	Yes	Yes	Yes	Yes
Administrative UI security (https://docops.ca.com/display/casso127/Protect+the+Administrative+UI+with+CA+Single+Sign-On) allows the Administrative UI to be protected by CA SSO authentication.	Yes	Yes	Yes	Yes
Agent discovery (https://docops.ca.com/display/casso127/Agent+Discovery) allows you to view agent-specific details such as version, state of operation and agent configuration objects within the Administrative UI. You can also view a list of agents that are deployed on various hosts in your enterprise and delete the unwanted agent instance entries from the list.	Yes	Yes	Yes	Yes

Administration and Supportability	12.51*	12.52*	12.6*	12.7
Administration workspaces (https://docops.ca.com/display/casso127/Create+an+Administrator) enables fine-grained delegation of CA SSO tasks, which define their administrative authority (https://docops.ca.com/display/casso127/Administrator+Use+Cases).	Yes	Yes	Yes	Yes
Integrated advanced password services (https://docops.ca.com/display/casso127/Advanced+Password+Services+Capabilities) provide a comprehensive set of password-management capabilities that extend beyond what basic password service provides.	Yes	Yes	Yes	Yes
Federation partnership management (https://docops.ca.com/display/casso127/Partnership+Federation) was enhanced with a wizard-driven approach for creating, updating, suspending, and deleting federation partnerships. The federation UI was also consolidated with Administrative UI to provide a single interface for managing the entire CA SSO environment.	Yes	Yes	Yes	Yes
Federation administrative scoping provides additional flexibility and fine-grained access control over privileges to manage federated partnerships (https://docops.ca.com/display/casso127/Partnership+Federation).	Yes	Yes	Yes	Yes
Expanded performance management support enables integration with CA Application Performance Management (CA APM) (https://docops.ca.com/display/casso127/Integration+with+CA+Application+Performance+Management) with the CA Access Gateway to allow you to monitor the performance of the embedded gateway Web Agent.	Yes	Yes	Yes	Yes
Expanded Agent Discovery support improves the visibility into the number and configuration of CA Access Gateway instances in the CA SSO environment.	Yes	Yes	Yes	Yes
Administrative UI for CA Access Gateway (https://docops.ca.com/display/casso127/CA+Access+Gateway+Configuration) simplifies the **configuration** (https://docops.ca.com/display/casso127/CA+Access+Gateway+Configuration)and management (https://docops.ca.com/display/casso127/CA+Access+Gateway+Management) of the access gateways.	Yes	Yes	Yes	Yes
Multiple access gateway instance (https://docops.ca.com/display/casso127/Install+CA+Access+Gateway) support allows you to host multiple instances of the gateway on the same server using group configuration.	Yes	Yes	Yes	Yes
Enhanced search enables administrators to search for resources, roles, and responses.	Yes	Yes	Yes	Yes
Attribute management provides the ability to select attributes from the session store (https://docops.ca.com/display/casso127/How+To+Add+Session+Attributes+to+an+Assertion)for inclusion in a SAML assertion or HTTP responses.	Yes	Yes	Yes	Yes
Assertion attribute logging allows administrators to record any assertion attributes used in transactions to the policy server logs (https://docops.ca.com/display/casso127/Enhanced+Auditing).	Yes	Yes	Yes	Yes