

Upgrading CA Single Sign-On



CA Single Sign-On (formerly CA SiteMinder) 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 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 TCO

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

Features—Authentication, Authorization and Session Management—WAM	12.5*	12.51*	12.52*
Dynamic (Ajax) application support enables CA Single Sign-On to provide authentication and authorization decisions for Ajax-based applications.	✓	✓	✓
Risk-aware authorization decisions improves the ability for CA Single Sign-On to make risk-aware authorization decisions throughout a user’s session.	✓	✓	✓
Expanded HTTP method support in CA Single Sign-On policies expands the product’s ability to provide authorization control for applications.	✓	✓	✓
CA Directory as a session store improves CA Single Sign-On integration with Directory by providing support for CA Directory to act as a session store. With free use of CA Directory, customers can leverage its fast performance.	✓	✓	✓
CA Identity Manager access roles in policies enables policy-based access controls using CA Identity Suite roles, which simplifies the use of the two products together and provides improved access control.	✓	✓	✓
Improved password policy integration with Microsoft® Active Directory® enhances Basic Password Services to recognize the error code that Active Directory sends when a password cannot be reused, so that the Policy Server can return the password reuse message to the end user.	✓	✓	✓
WebDav support in Secure Proxy Server (SPS) enables CA Single Sign-On to extend authentication and authorization to additional classes of applications using this protocol.	✓	✓	✓

* 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—WAM (continued)

Session linker incorporated in SPS links the CA Single Sign-On session to session tokens of other applications that CA Single Sign-On provides protection for, such as IBM® WebSphere® and SAP, which protects the tokens of these application from being hijacked. This capability improves the security of these applications and the IT infrastructure as a whole.	✓	✓	✓
Support for Application Server Agents with SPS so you can use Application Server Agents with the SPS instead of a web agent. By using SPS for this purpose, you can reduce the number of web agents, cost of management and simplify your single sign-on (SSO) infrastructure.	✓	✓	✓
IWA support via SPS enables you to remove other SSO IIS Web Agents that may have only been being used to provide the IWA support in your SSO infrastructure.	✓	✓	✓
Enhanced proxy rules via SPS provides the ability to support more access management use cases.	✓	✓	✓
Open format cookies enable you to design your web applications to consume these lightweight, open-format cookies to achieve SSO via a simpler process than deploying a full CA Single Sign-On Web Agent.	X	✓	✓
Web services interface for authentication and authorization creates another flexible method for you to integrate applications to request authentication and authorization services from CA Single Sign-On.	X	✓	✓
Required authentication for every access of a specific resource lets administrators now specify resources within applications that require users to authenticate again with their credentials before access is granted.	X	✓	✓
Enhanced Session Assurance with DeviceDNA™ is a patent-pending feature that helps prevent unauthorized users from hijacking legitimate sessions by stealing cookies	X	X	✓
Link presence of x.509 key to session	X	X	✓
Improved password policy integration with CA Directory	X	X	✓
Authentication, Authorization and Session Management— Federation			
CA Directory as a session store. In federation use cases, the session store can maintain attributes from Security Assertion Markup Language (SAML) assertions or OAuth tokens for use in authorization decisions.	✓	✓	✓
Support for authentication context provides the ability for an SP to enforce a stronger form of user authentication before providing access to a resource.	✓	✓	✓
Ability to enforce user consent. In a federation transaction, user consent of the identity information being provided from the IdP to the SP can be required. That requirement can be set by CA Single Sign-On when acting as either an SP or and IdP.	✓	✓	✓
Service provider attribute mapping helps a service provider offer an application to multiple identity providers.	✓	✓	✓
<i>* some of these enhancements introduced in SPs and CRs on these releases</i>			
CHART KEY:			
<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #004a7c; margin-right: 5px;"></div> Expanding support for enabling secure business through new applications and new use cases </div>			
<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #00a0c0; margin-right: 5px;"></div> Simplifying use and lowering TCO </div>			

Authentication, Authorization and Session Management— Federation (continued)

Dynamic user provisioning interface provides support for just-in-time provisioning of user information and enables organizations to more quickly support new users needing access to SP-side applications.	✓	✓	✓
Service Level Objective (SLO)/Simple Object Access Protocol (SOAP) enables the use of CA Single Sign-On for federated SSO with more applications.	✓	✓	✓
Java™ and .Net SDK support broadens the application integration capabilities of CA Single Sign-On for open format cookies and federation transactions.	✓	✓	✓
OAuth RP support for Google and Facebook provides out-of-the-box functionality to configure CA Single Sign-On to validate OAuth tokens provided by Google and Facebook.	X	✓	✓
Browser SSO to Office 365™ via WS-Federation offers support for browser-based access via the WS-Federation protocol.	X	✓	✓
SAML attribute query enables CA Single Sign-On to support more applications when the initial assertions passed don't include all the necessary attributes to successfully complete federated SSO transaction.	X	✓	✓
Attribute transformation when generating an assertion. Claims transformation manipulates claims during a federated SSO transaction, which help customize the attributes and improve the user experience at a partner.	X	✓	✓
Persisting SAML attributes. From the session store, the system can add attributes to an assertion to customize the requested application.	X	✓	✓
OAuth RP support for Twitter, LinkedIn, Microsoft Live. Negative assertion support expanded the out-of-the-box ability to configure the product to validate OAuth tokens provided by LinkedIn, Microsoft Live and Twitter.	X	X	✓
Enhanced NameID support enables the deprovisioning of an individual user from a partnership	X	X	✓
Thick client support for SSO to Office 365. Expanded support for SSO to Office 365 to support thick clients such as Excel®, PowerPoint® and Word was introduced with support for 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	✓
Notification to service provider of failed authentication. The administrator can configure a partnership to notify the service provider when a user fails to authenticate, so the service provider can determine appropriate action.	X	X	✓
Enhanced social sign-on lets users access a federated resource using their social networking credentials instead of the federation system credentials.	X	X	✓
IWA authentication for SSO via thick clients to Office 365	X	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			
Hardware load balancer between policy server and agents to expose multiple policy servers to agents through one or more virtual IP addresses.	✓	✓	✓
Key store moved to the policy store replaces the need for multiple, local SMKey databases with a single certificate data store. All policy servers that share a common view into the same policy store have access to all certificates and keys in the environment.	✓	✓	✓
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.	✓	✓	✓
CA SSO authentication protection for the admin UI improves the security around the administration of CA Single Sign-On.	✓	✓	✓
Agent discovery allows you to view agent-specific details such as version, state of operation and agent configuration objects. 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. CA Single Sign-On administrators are assigned rights to one or more security feature categories that define their administrative authority in the Administrative UI, such as managing authentication schemes.	✓	✓	✓
Integrated packaging of APS provides a comprehensive set of password management capabilities that extend beyond what basic password services provides.	✓	✓	✓
Wizard-driven UI for federation partnerships was enhanced with a wizard-driven approach for creating, updating, suspending and deleting federation partnerships.	✓	✓	✓
Integrated installation of federation administration with base SSO install provides a single administration UI for managing a combined SSO platform.	✓	✓	✓
Administration scoping and delegation for managing federation partnerships provides additional flexibility and control over which administrator has rights for managing which partnerships.	✓	✓	✓
Performance management support in SPS allows integration with CA Application Performance Manager, letting you monitor the data performance of the SPS web agent.	✓	✓	✓
Agent discovery supported in SPS improves the visibility of the SSO administrator into the number and configuration of SPS instances in their environment.	✓	✓	✓
Administrative UI for SPS simplifies the use of SPS.	✓	✓	✓
Ability to host and manage multiple instances of SPS on the same server. Group configuration lets you group the hosts configured to a policy server, so you can manage the configuration of the host servers using any host in the group.	✓	✓	✓
Enhanced searching capabilities for resources, roles, responses.	X	✓	✓
Admin UI enhancements to provide the ability to select attributes from the session store to include in SAML assertion or HTTP responses.	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. Policy server administrators can now record any assertion attributes used in transactions to the policy server logs.	X	✓	✓
Enhanced user disambiguation with IWA and Kerberos authentication improves and simplifies the use of the Kerberos and IWA authentication schemes.	X	X	✓
Detailed logging of federation transaction flows. If a 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 who need access to RP-side applications.	X	X	✓
Certificate list cross references partnerships	X	X	✓
Enhanced sorting and searching in the domain policies page of the administrative user interface	X	X	✓
Packaged CA Remote Engineer delivered by CA Single Sign-On 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 capability to repair policy objects simplifies the identification and cleanup of invalid policy objects, helping to ensure simpler upgrade and reliability.	X	X	✓
Improved algorithm for capturing trace logs improves the performance and reliability for gathering detailed tracing data when troubleshooting a service problem.	X	X	✓
Multiple ACOs for IIS Web Agent allow organizations that have shared Microsoft IIS servers to use different settings for each IIS website, enabling more-efficient use of hardware systems. This also makes configuration easier by providing a greater degree of flexibility and isolation between applications.	X	X	✓
Turn off authorization calls for web agents produces faster website response times and reduced network traffic on web servers.	X	X	✓
Platforms and Internals			
Operating system support for the policy server—Red Hat 6	✓	✓	✓
Standardized internationalization and localization extended to additional languages , including French, German, Italian, Spanish, Korean and Brazilian Portuguese (in addition to the long-standing Japanese translation).	X	✓	✓
Syslog support for audit data. Administrators can direct policy server audit data to the syslog on supported UNIX® operating environments.	X	✓	✓
Recent performance improvements specifically focused on administration of large policy stores and session store.	X	X	✓
Performance improvements across authentication, authorization and administration. Removing performance bottlenecks enables organizations to support more access control with fewer system resources, providing ROI improvements.	At each release		
<i>* some of these enhancements introduced in SPs and CRs on these releases</i>			
CHART KEY:			
 Expanding support for enabling secure business through new applications and new use cases			
 Simplifying use and lowering TCO			

Licensing			
Free use of CA Directory as a policy store, session store, key store. Paid licenses are still required if you want to use CA Directory as a user store.	✓	✓	✓
SPS product license incorporated into base CA SSO license price. New customers that first purchased CA SSO from 12.51 onward, SPS is offered free of charge as part of the base CA SSO license. For existing customers that have owned CA SSO prior to the GA of 12.51, SPS can be used free of charge if the customer never purchased SPS.	X	✓	✓
Unlimited federation is included for all licensed CA Single Sign-On users	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

To learn more about how these new releases are delivering more business value, watch these release training videos:

- [CA Single Sign-On r12.52—Extending Your Security Investment](#)
- [The new CA SSO \(formerly SiteMinder\) r12.51 release](#)



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.