PRODUCT SUPPORT MATRIX

CA Single Sign-On 12.8

Last Modified: September 23, 2019 (Changes are highlighted in green)

Table of Contents

1 At a Glance

Welcome to CA Technologies Single Sign-On 12.8 Platform Support Matrix. This document describes a variety of software components, operating system, database, directory and other 3rd party software components supported for this release. The document also highlights additional support policies, guidelines and clarifications as appropriate for the different components.

2 Single Sign-On Server Components

This section lists combinations of platform choices supported for the CA Single Sign-On server components, including the following components:

- CA Single Sign-On Policy Server
- CA Single Sign-On Policy Server SDK
- CA Administrative User Interface

2.1 Operating System for Policy Server, SDK & Access Gateway

The following table lists CA Single Sign-On server components and Access Gateway support for Operating Systems [1,2]:

CA Single Sign-On Component	Windows Server [3,4]	Red Hat [5]	Solaris
Policy Server 64 bit [6,7,8]	2016, 2012 R2	7 6	
Policy Server SDK 64 bit	2016, 2012 R2	7 6	

CA Single Sign-On Component	Windows Server [3,4]	Red Hat [5]	Solaris
Access Gateway 64 bit	2016, 2012 R2	7 6	11.x

Applicable Support Notes:

1. Hardware requirements:
   a. Windows Server on x64 (Intel and AMD).
   b. Red Hat Enterprise Linux on x64 (Intel and AMD).

2. 64-bit Support: Single Sign-On 64-bit Operating Systems are supported.

3. On Windows 2012R2, Server Standard/Enterprise Essentials/Web Datacenter / Foundation Editions are supported.

4. On Windows 2016, Server Standard/Enterprise Essentials/Web Datacenter Editions are supported.

5. Red Hat AS, Red Hat ES, Red Hat Enterprise Linux and Red Hat Enterprise Linux Advanced Platform are supported with all Red Hat updates. Any problems reported will be fixed on the latest Red Hat update. Security Enhanced Red Hat Linux is supported, please see vendor's documentation for setup instructions to enable third-party processes (such as Single Sign-On) to run on the system.

6. Single Sign-On Policy Server includes a Scripting Interface (or Command Line Interface) that uses Perl scripts to configure and manage policy stores. The installation program installs a full version of Perl. The Interface is available on all platforms supported by the Policy Server.

7. Building custom authentication schemes on Linux: When building Single Sign-On custom authentication schemes, or any other custom-built components, you must use GCC version 3.4.6 and above.

8. When building custom components for the Policy Server (e.g. authentication schemes) they must be compiled as a 64-bit binary.

2.2 Operating System for CA Single Sign-On Administrative User Interface

1. Administrative User Interface with embedded Application Server is supported on operating systems supported by policy server.
2. Browser support for the administrative User Interface

    a. Internet Explorer – IE11 (in "compatibility mode").
    b. Microsoft Edge
    c. Safari – supported with Safari version 9.1.2
    d. Firefox - supported with latest versions, last tested with 59.
    e. Google Chrome – supported with latest versions, last tested with 65.

2.3 Database and Directory Systems

The following table lists Database and Directory systems that CA Single Sign-On supports for various data stores:

Data Store System [1]	Version	Policy Store	Session Store	User Store	Basic Password Services	Admin UI Store	Audit Store
CA Directory Server	12.x, 14.0, 14.1	Yes	12 SP7 or later	Yes	Yes	Yes	
CA LDAP Server for z/OS RACF	15			Yes			
CA LDAP Server for z/OS ACF-2	15			Yes			
CA LDAP Server for z/OS Top Secret	15, 16			Yes			

Data Store System [1]	Version	Policy Store	Session Store	User Store	Basic Password Services	Admin UI Store	Audit Store
IBM Tivoli Directory Server	6.3	Yes		Yes	Yes	Yes	
	6.4	Yes		Yes	Yes	Yes	
IBM DB2 UDB	11.1	Yes	Yes	Yes	Yes		Yes
	10.5	Yes	Yes	Yes	Yes		Yes
	10.1	Yes	Yes	Yes	Yes		Yes
Microsoft Active Directory (AD)[2]	2016	Yes		Yes	Yes	Yes	
	2012 R2	Yes		Yes	Yes	Yes	
	2012	Yes		Yes	Yes	Yes	
Microsoft Active Directory Lightweight Directory Services (LDS)[2]	2016	Yes		Yes	Yes	Yes	
	2012, 2012 R2	Yes		Yes	Yes	Yes	
Microsoft AD Global Catalog[2]	2016, 2012R2			Yes		Yes	
Microsoft SQL Server Including cluster [2,3]	2016	Yes	Yes	Yes	Yes	Yes	Yes
	2014	Yes	Yes	Yes	Yes	Yes	Yes
	2012	Yes	Yes	Yes	Yes	Yes	Yes

Data Store System [1]	Version	Policy Store	Session Store	User Store	Basic Password Services	Admin UI Store	Audit Store
Novell eDirectory	9.0, 8.8.x	Yes		Yes	Yes	Yes	
OpenLDAP	2.4	Yes		Yes	Yes	Yes	
Oracle Directory Server Enterprise Edition	11gR1, 11gR1-SP1, essentially 11.1.1.x	Yes		Yes	Yes	Yes	
Oracle Internet Directory	12c, 11gR1	Yes		Yes	Yes	Yes	
Oracle MySQL Enterprise Server	5.x	Yes	Yes	Yes	Yes		Yes
Oracle RDBMS[4]	12c, 12c R1, 12c R2	Yes	Yes	Yes	Yes	Yes	Yes
Oracle RAC	12c	Yes	Yes	Yes	Yes	Yes	Yes
	12cR2			Yes	Yes		
Oracle Unified Directory (OUD)	11gR2	Yes		Yes			
	12c	12.8.02		12.8.02			
Oracle Virtual Directory (OVD)	11gR1	Yes		Yes			

Data Store System [1]	Version	Policy Store	Session Store	User Store	Basic Password Services	Admin UI Store	Audit Store
Red Hat Directory Server	10.x	Yes		Yes	Yes	Yes	
	9.x	Yes		Yes	Yes	Yes	
PostgreSQL	9.3, 9.4, 9.6	Yes	Yes	Yes	Yes		Yes

Applicable Support Notes:

1. Information on CA Single Sign-On Policy Stores multi-master replication mode is available in the Product Documentation.
2. Microsoft Windows Server and for Microsoft SQL Server, service packs (e.g., SP1, SP2) are supported in addition to the base releases shown in the matrix.
3. The following Microsoft SQL Server Editions are supported: Standard Edition, Enterprise Edition and Datacenter Edition.
4. The following Oracle RDBMS Editions are supported: Standard Edition One, Standard Edition, and Enterprise Edition.

2.4 Java Virtual Machine (JVM)

Review this section carefully. The Java support has been changed as of the release of 12.8.03.

The following table lists the Java Virtual Machine (JVM) support requirements for release **12.8.03**:

CA Single Sign-On Component	Java Runtime Environment [1,2]
Single Sign-On Policy Server	AdoptOpenJDK 1.8.212 (or later updates on 1.8.x) 64 bit
Policy Server SDK 64 bit	AdoptOpenJDK 1.8.212 (or later updates on 1.8.x) 64 bit
Access Gateway	AdoptOpenJDK 1.8.212 (or later updates on 1.8.x) 64 bit

The following table lists the Java Virtual Machine (JVM) support requirements for 12.8.02 lower numbered versions:

CA Single Sign-On Component	Java Runtime Environment [1,2]
Single Sign-On Policy Server	Oracle JDK 1.8 (or later updates on 1.8.x) 64 bit
Policy Server SDK 64 bit	Oracle JDK 1.8 (or later updates on 1.8.x) 64 bit
Access Gateway	Oracle JDK 1.8 (or later updates on 1.8.x) 64 bit

Applicable Support Notes:

1. Please note that Java Developer Kit (JDK) is required and not just the Java Runtime Environment (JRE) package.

2. Listed JVM build or above on the same series are supported.

3 Single Sign-On Optional Components

3.1 One View Monitor

One View Monitor component can be deployed on Tomcat 8.5.x and can be run on the Operating Systems supported by the Policy Server (noted in section 2.1).

3.2 Advanced Password Services (APS)

APS Policy Server Components:

APS components that run on the Single Sign-On Policy Server are supported on the Operating Systems supported by the Policy Server (noted in section 2.1)

APS Database and Directory:

Data Store	Version
CA Directory	12.x, 14.0, 14.1
Microsoft Active Directory	2012R2, 2016
	2012R2 LDS, 2016 LDS
Microsoft SQL Server	2012, 2014, 2016
Oracle RDBMS	12c, 12c R1, 12c R2

4 CA Security Cross Product Compatibility

4.1 Policy Server and Agents Compatibility

CA Single Sign-On Policy Server 12.8 supports previous versions of Agents and Access Gateways (previously called Secure Proxy Server) with the following caveats:

- The 12.8 Single Sign-on Policy Server includes changes initially delivered in the 12.6 Policy Server that were made to the design of the Enhanced Session Assurance with DeviceDNA™ feature. That redesigned feature requires and will only work with the 12.6 or higher numbered versions of the Access Gateway. NOTE this restriction only applies to the Session Assurance feature. All other usage patterns (e.g. reverse proxy, federation, Rest interface, session linking) are supported with the 12.8 Policy Server in combination with earlier versions of the Access Gateway.
- Any 6.x versions of Web Agents, Access Gateways (previously called Secure Proxy Server), ERP Agents, ASA Agents, and 5.x versions of ERP Agents that are not beyond their end-of-service date do not support IPv6 or FIPS Mode (and can only connect to 12.8 Policy Server in FIPS Compatibility Mode).
- Web Agent, Access Gateway, ERP Agent and ASA Agent versions prior to r12.0 SP3 cannot be installed on the same machine as a r12.6 (or higher numbered) Policy Server.
- The CA Single Sign-On 12.8 release provides backward compatibility between Single Sign-On Policy Server and earlier versions of the Web Agent Option Pack (WAOP) back to Single Sign-On r12 SP3 CR9. WAOPs prior to r12 SP3 CR9 are not supported with 12.8 Policy Servers
- Session Linker is deployed by the Policy Server Installer, starting from 12.7 release.

4.2 CA Single Sign-On Web Services Security Compatibility

As of the release of CA Single Sign-On 12.51 and later, Single Sign-On Web Services Security functionality is incorporated in the base Single Sign-On Policy Server and Single Sign-On Administrative UI. As a result the supported operating systems for the CA Single Sign-On Web Services Security Policy Server are the same as the operating systems listed for Single Sign-On Policy Server (as noted in section 2.1) and the Single Sign-On Administrative UI. The supported operating systems for CA Single Sign-On WSS Agents can be found on the platform support matrix for the Single Sign-On Web Services Security product page that can be located from this root page. Locate the matrix on the product page at this link: https://support.ca.com/irj/portal/anonymous/phpsbpldgpg

4.3 CA Security Product Compatibility

The following table lists supported integrations between CA Single Sign-On and other CA Products:

Product	Version	CA Single Sign-On Policy Server Operating System
CA Federation Standalone (previously CA Federation Manager)	12.52	Windows Server 2016, 2012R2 RHEL 6,7
CA Identity Manager/Suite	14.1, 14.0, 14.1,12.6 SP4 or later only It is not recommended to place CA Single Sign-On and CA Identity Manager on the same system	Windows Server 2016, 2012R2 RHEL 6,7
CA Advanced Authentication (CA Strong Authentication, CA Risk Authentication) CA Adapter	8.x, 9.0, 9.1	Windows Server 2016, 2012R2 RHEL 6,7

5 Third-Party Product Compatibility

The following table lists supported third-party products:

Product	Version
RSA Authentication Manager[1]	8.3 8.2.x 8.1.x 8.0.x

Applicable Support Notes:

1. For RHEL 7 platform, note that RSA SDK support is from RHEL 7.1 onwards. Hence policy server needs to be deployed on RHEL 7.1 or above, to use RSA SecurID authentication.

6 Support Considerations

6.1 IPV6 Support Statement

CA Single Sign-On supports IPv6 with the sole exception of communication to the Advance Password Services component for all communication unless the 3rd party software component that Single Sign-On is communicating with does not support IPv6.

6.2 Virtualized Environment Support

Single Sign-On follows the general CA Policy for Virtualization noted below: http://www.ca.com/us/services-support/ca-support/ca-support-online/product-content/recommended-reading/announcements/ca-support-statement-for-virtualization.html

6.3 Internationalization Support

CA Single Sign-On 12.8 has been internationalized. This means every component of the Single Sign-On product family that carries the 12.8 version number or a later version number has been internationalized and will run on localized versions of operating systems, support localized applications, and localized data. Please see the product documentation for information about what parts of the Single Sign-On family have been translated.

6.4 Reasonable Commercial Effort Statement

CA Technical Support will make a reasonable commercial effort to troubleshoot and/or resolve customer support requests that involve the use of currently supported versions of CA Single Sign-On on or with “unsupported” platforms as follows:

CA Technical Support will accept support incidents (support requests) involving a software platform of a combination of software platforms that is not officially supported per the then-current CA published platform support matrices. CA will troubleshoot the issue up to the point that CA has reason to believe that the problem is related to the use of software that is not specified in a then-current platform supported matrix. At such point, CA shall require that the customer reproduce the problem on a fully supported combination of platforms before CA proceeds in troubleshooting the incident.

Linux Reasonable Commercial Effort Statement:

This Support Statement applies to CA Single Sign-On that offers documented support for one or more Linux Reference Platforms. CA strives to meet our clients’ diverse and ever changing needs. CA products support and manage many of today's leading platforms, operating systems and applications across the IT enterprise. A Linux Reference Platform is a specific version of a particular Linux variant, such as Red Hat Enterprise Server 6, which is used in CA development, QA, and Support, and is documented as a supported environment in which to run CA Single Sign-On. To verify the Linux Reference Platforms supported for CA Single Sign-On, review the system requirements section of the respective product documentation, or check with CA Support. Many of our clients use variants of the Linux operating system as their production operating system platform, for example Oracle Enterprise Linux, SUSE, etc. Some of those Linux variants claim compatibility (compatibility modes) with CA Single Sign-On supported Linux Reference Platforms.

Note: CA does not test every possible configuration of CA Single Sign-On running on the many Compatible Linux Variants available and cannot certify specific client configurations.

To facilitate a quick resolution and isolate the root cause of any potential product issue encountered running on Compatible Linux Variants, CA is establishing the following support protocol for CA Single Sign-On operated in these environments:

- The current GA version of a Linux Reference Platform and the prior major version of that environment are supported. Any exceptions will be noted in respective product documentation.
- The client is responsible for properly configuring their Linux Variant to be compatible with a Linux Reference Platform supported by CA Single Sign-On.
- The client is responsible for having an active maintenance agreement for both their CA Single Sign-On and for the Compatible Linux variant.
- While CA does not require that clients recreate each issue on a Linux Reference Platform before contacting support, we can request that the client diagnose and troubleshoot specific issues without the Linux Variant "variable" through reproducing the issue on the Linux Reference Platform. CA will only do this when we have reason to believe the issue is directly related to the Compatible Linux Variant environment.
- While functional problems are rare under Compatible Linux Variants, problems may occur related to the third-party components embedded in applications, and those embedded products' support of Compatible Linux Variants may be limited or unavailable. Diagnosis and resolution of this class of problem may require the client to return to a Linux Reference Platform.
- Compatible Linux Variants are diverse; CA may require extra time to understand, collect data, troubleshoot and possibly reproduce reported issues.
- If CA Support cannot directly identify the root cause as a CA or a Compatible Linux Variant issue, client can open a support issue with their Compatible Linux Variant vendor and any other necessary third-party vendors to expedite the resolution of the issue. CA, the vendor(s), and the client will work together toward a quick resolution where there business relationship mechanism to do so. CA, Novell, and many other software vendors belong to the Technical Support Alliance Network (http://www.tsanet.org) that may be engaged by either CA or the Compatible Linux variant vendor if and when the need for a third-party arises as long as active

maintenance exists for the CA and third party vendor's product. Note if the customer does not have a Vendor support agreement for the Linux variant, there is no third party CA may work with.

- Any known issues with running CA Single Sign-On on specific Compatible Linux Variants will be noted in the respective product documentation.

6.5 Third-Party Products End of Support Statement

When a third-party product reaches the end of its primary, premier, production-phase or mainstream support (which is prior to, and distinct from optional, separately purchased, add-on extended support vendor support), CA will no longer provide explicit support / certification for that third-party product or any CA Single Sign-On components that interoperate with the third-party product.

Third-party products under optional, separately purchased, add-on extended vendor support are not used in development / release cycles of upcoming major releases OR minor releases like CR / SP. They are at best supported within our 'Reasonable Commercial Effort Statement', so as to help customers move to newer versions supported by CA Single Sign-On components. Examples of third-party products are: web server, application server, operating system, directory, database, etc.