Table of Contents

1   At a Glance

Last updated date: May 16th, 2018

This document identifies platform support for CA Privileged Access Manager versions 2.8, 3.0, 3.1 and 3.2. It is published on the CA Support website and is updated as platforms are added or removed. CA Privileged Access Manager is shipped as either a hardware or software based appliance, but in both cases the Operating System and Database is included with the software package. The information below references supported platforms for end-point Session Management, Credential Management or where applicable, the installation of ancillary agents (A2A Client, Socket Filter Agent or CA PAM Workstation Client) which are required for certain features of CA Privileged Access Manager. Note that CA PAM Workstation Client is the primary access method to CA PAM. The only browser option is Microsoft Internet Explorer 11 as this remains the only browser with NPAPI support. If using IE11, Java 8u-latest must be installed on the desktop.

2   Session and Credential Management Platform Support

2.1 Operating System Platforms	V2.8.x	V3.0.x	V3.1.x	V3.2.x
Centos 7.0	✓	✓	✓	✓
Centos 7.2	✓	✓	✓	✓
Fedora™ 23	✓	✓	✓	✓
IBM® AIX 7.3	✓	✓	✓	✓
Microsoft® Windows 2008 R2	✓	✓	✓	✓
Microsoft® Windows 2012 R2	✓	✓	✓	✓
Microsoft® Windows 7	✓	✓	✓	✓
Microsoft® Windows 8.1	✓	✓	✓	✓
Microsoft® Windows 10	✓	✓	✓	✓
Microsoft® Windows 2016			✓	✓
Oracle® Solaris 10	✓	✓	✓	✓
Oracle® Solaris 11.0	✓	✓	✓	✓
Red Hat® Enterprise Linux 6.6	✓	✓	✓	✓
Red Hat® Enterprise Linux 7.0	✓	✓	✓	✓
Red Hat® Enterprise Linux 7.2	✓	✓	✓	✓
SuSE® Linux Enterprise Server 11 SP3	✓	✓	✓	✓

2.2 Databases (as Target Applications)[1]	V2.8.x	V3.0.x	V3.1.x	V3.2.x
IBM® DB2 v10.5	✓	✓	✓	✓
Microsoft® SQL Server 2008 R2	✓	✓	✓	✓
Microsoft® SQL Server 2012 R2	✓	✓	✓	✓
Microsoft® SQL Server 2014	✓	✓	✓	✓

---

[1] IBM® DB2 is an OS credential (use Unix connector. See product documentation)

Oracle® 11g	✔	✔	✔	✔
Oracle® 12c	✔	✔	✔	✔
Oracle® MySQL 5.7	✔	✔	✔	✔

2.3 Network Devices [2]	V2.8.x	V3.0.x	V3.1.x	V3.2.x
Cisco™ ASA	✔	✔	✔	✔
Cisco™ IOS	✔	✔	✔	✔
Cisco™ TACACS+ Server	✔	✔	✔	✔
PaloAlto PAN Server 6	✔	✔	✔	✔
PaloAlto Devices (Layer 3, Option C configuration)	✔	✔	✔	✔
*Devices with *nix Operating Systems using SSHv2 connection*	✔	✔	✔	✔

2.4 Mainframe[3,4]	V2.8.x	V3.0.x	V3.1.x	V3.2.x
CA ACF2™ r15	✔	✔	✔	✔
CA TopSecret® r15	✔	✔	✔	✔

2.5 Directories	V2.8.x	V3.0.x	V3.1.x	V3.2.x
CA® Directory v12	✔	✔	✔	✔
Microsoft® Active Directory[5]	✔	✔	✔	✔
Red Hat® Enterprise Linux 389 [6]	✔	✔	✔	✔
LDAP v3 compliant directories [7]	✔			

2.6 Cloud & Virtualization Platforms	V2.8.x	V3.0.x	V3.1.x	V3.2.x
Amazon Web Services™ Admin web console access	✔	✔	✔	✔
Microsoft® Office 365 Admin console access	✔	✔	✔	✔
VMware® vCenter 5.x	✔	✔	✔	✔
VMWare® NSX for vSphere	✔	✔	✔	✔

---

[2] As Target Applications. Typically Network devices use SSH protocol for User session establishment (use Unix connector. See product documentation)

[3] Requires CA LDAP for Mainframe System z

[4] Transparent Login functionality for Mainframe not supported

[5] For an any supported Windows Server

[6] When installed on a supported Red Hat Enterprise Linux Server

[7] When installed on a supported *nix Server

2.7 Web/Application Servers	V2.8.x	V3.0.x	V3.1.x	V3.2.x
Apache Tomcat 7	✓	✓	✓	✓
Apache Tomcat 8	✓	✓	✓	✓
IBM® Websphere	✓	✓	✓	✓
Oracle® Weblogic	✓	✓	✓	✓

2.8 Others requiring 3rd party license	V2.8.x	V3.0.x	V3.1.x	V3.2.x
Sybase 15	✓	✓	✓	✓

2.9 CA Threat Analytics (for PAM)	V2.8.x	V3.0.x	V3.1.x	V3.2.x
CA Threat Analytics (for PAM) v2.0	✓	✓	✓	✓
CA Threat Analytics (for PAM) v2.2	✓	✓	✓	✓

2.10 IT Service Management Systems	V2.8.x	V3.0.x	V3.1.x	V3.2.x
CA Service Desk Manager 12.6	✓	✓	✓	
CA Service Desk Manager 12.7	✓	✓	✓	
CA Service Desk Manager 12.9	✓	✓	✓	
CA Service Desk Manager 14.1	✓	✓	✓	✓
CA Service Desk Manager 17.0				✓
BMC Remedy 8.1	✓	✓	✓	✓
BMC Remedy 9.1				✓
HP Service Manager 9.32	✓	✓	✓	✓
HP Service Manager 9.41				✓
Salesforce Service Cloud (Winter 2015)	✓	✓	✓	✓
ServiceNow (Eureka)	✓	✓	✓	
ServiceNow (Fuji)	✓	✓	✓	
ServiceNow (Geneva)	✓	✓	✓	
ServiceNow (Instanbul)				✓
ServiceNow (Jakarta)				✓

3   CA PAM Workstation Client

The CA PAM Workstation Client enables you to log in to CA Privileged Access Manager and perform administrator and end-user activities without the use of a customer-installed web browser and Oracle Java engine, removing the maintenance required to keep Java and browser configurations compatible with CA PAM. You can run any CA PAM connection applets and provide a complete substitute for the traditional CA PAM GUI.

The client does not interfere in any way with traditional GUI access – both methods can be used from the same workstation. However, From January 1st 2017, the only browser option is Microsoft Internet Explorer 11 (the only browser still with NPAPI support which is required for the applets). If using IE11,

Java 8u-latest must be installed on the desktop (Oracle Java 7 is EoL for public updates).

You can download a client version compatible with your workstation OS types and install from a button on the CA PAM GUI login page. The embedded JRE is downloaded with the client but CA PAM-served JARs download at runtime.

PAM v2.8.3 fixed multi-user access via a published App. (eg Citrix Store front or RDP).

3.1 CA PAM Workstation Client (End User Desktop Support)	V2.8.x	V3.0.x	V3.1.x	V3.2.x
Microsoft® Windows 7, 8.1, 10	✓	✓	✓	✓
Microsoft® Windows 2012 R2, 2016			✓	✓
RHEL 7.3 x64	✓	✓	✓	✓
Apple macOS (El Capitan, Sierra)	✓	✓	✓	✓

4   Mobile support for CA PAM

CA Privileged Access Manager offers limited support for mobile devices. The CA PAM browser user interface has been optimized for password view requests and password check in and check out operations for mobile devices.

4.1 Mobile Support			PAM
Mobile Device	**Operating System**	**Browser**	**V3.2x**
iPhoneX	iOS 11	Safari	✓
iPhone8	iOS 11	Safari	✓
iPad Pro 12.9	iOS11	Safari	✓
iPad Pro 10.5	iOS11	Safari	✓
Samsung Galaxy 8	Android 7 (Nougat)	Chrome v.64.0.3282	✓
Samsung Galaxy 7	Android 7 (Nougat)	Chrome v.64.0.3282	✓

5   CA PAM App2App Client

App2App integration allows administrators to provide authorization for applications to access privileged credentials for application to application transactions. An App2App client is installed on the Request server where the requesting application(s) resides and has a variety of security checks to maintain authorization control. Multiple programming and scripting languages can be used (see product documentation for integration details).

5.1 CA PAM App2App Client	V2.8.x	V3.0.x	V3.1.x	V3.2.x
AIX 6	✓	✓	✓	✓
AIX 7	✓	✓	✓	✓
Microsoft® Windows 2008 R2	✓	✓	✓	✓
Microsoft® Windows 2012 R2	✓	✓	✓	✓

Microsoft® Windows 2016			✓	✓
Red Hat Enterprise Linux 6	✓	✓	✓	✓
Red Hat Enterprise Linux 7	✓	✓	✓	✓
Solaris 10	✓	✓	✓	✓
Solaris 11	✓	✓	✓	✓
SuSE® Linux 11sp2 (64bit)	✓	✓	✓	✓

5.2 CA PAM App2App languages	**V2.8.x**	**V3.0.x**	**V3.1.x**	**V3.2.x**
Java	✓	✓	✓	✓
C++	✓	✓	✓	✓
C	✓	✓	✓	✓
C#	✓	✓	✓	✓
PHP	✓	✓	✓	✓
Python	✓	✓	✓	✓
JavaScript	✓	✓	✓	✓
Perl	✓	✓	✓	✓
Korn Shell	✓	✓	✓	✓
C Shell	✓	✓	✓	✓

6   CA PAM Socket Filter Agent

Installed on an Endpoint, the Socket Filter Agent is use to provide lateral containment (i.e. preventing administrators from "leap frogging" to another server).

6.1 CA PAM SFA Client	**V2.8.x**	**V3.0.x**	**V3.1.x**	**V3.2.x**
Unix, Linux	✓	✓	✓	✓
AIX 6	✓	✓	✓	✓
AIX 7	✓	✓	✓	✓
Microsoft® Windows 2008 R2	✓	✓	✓	✓
Microsoft® Windows 2012 R2	✓	✓	✓	✓