Privileged Access Security System Requirements

Version 10.4

Including:
Privileged Identity Management Suite
Privileged Session Management Suite

PASSR-10-4-0-2

Table of Contents

Recommended Server Specifications

The following tables summarize the recommended hardware and software specifications for the required servers when implementing CyberArk's Privileged Access Security (PAS) solution. These hardware specifications are based on the entry level industry standard for small to mid-range servers.

For installation on a VM based environment, the requirements can be customized based on customer needs, according to the CyberArk server requirements.

Vault and DR Vault servers

The following table lists the recommended specifications for standalone Vault servers and standalone DR Vault servers.

Specifications

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
▪ Quad core processor (Intel compatible) ▪ 8GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM ▪ Additional storage for PSM (optional)	▪ 2X Quad core processor (Intel compatible) ▪ 16GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM ▪ Additional storage for PSM (optional) [1]	▪ 2X Eight core processors (Intel compatible) ▪ 32GB RAM ▪ Two 250GB SAS hot-swappable drives (15K RPM) ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM ▪ Additional storage for PSM (optional) [1]	▪ 4X Eight core processors (Intel compatible) ▪ 64GB RAM ▪ Two 500GB SAS hot-swappable drives (15K RPM) ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM ▪ Additional storage for PSM (optional) [1]
Software prerequisites			
▪ Windows 2016 English Edition ▪ Windows 2012 R2 English/German version [2] ▪ Windows 2008 R2 SP1 (64-bit) English/German version [2] ▪ .NET Framework 4.5.2			

[1] For more information, refer to Privileged Session Manager®, page 40.

[2] Contact your CyberArk support representative for the most recent supported service pack requirements.

For security reasons, CyberArk recommends installing Vault instances on physical hardware.

Cluster Vault and Cluster DR Vault servers

The following table lists the recommended specifications for the Cluster Vault server and the Cluster DR Vault server [1] .

Specifications

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
▪ Quad core processor (Intel compatible) ▪ 8GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ 2X Network adapter (1Gb) ▪ DVD ROM ▪ SCSI/Fibre shared disk that supports the SCSI3 protocol ▪ Additional storage for PSM (optional) [2]	▪ 2X Quad core processor (Intel compatible) ▪ 16GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ 2X Network adapter (1Gb) ▪ DVD ROM ▪ SCSI/Fibre shared disk that supports the SCSI3 protocol ▪ Additional storage for PSM (optional) [2]	▪ 2X Eight core processors (Intel compatible) ▪ 32GB RAM ▪ Two 250GB SAS hot-swappable drives (15K RPM) ▪ RAID Controller ▪ 2X Network adapter (1Gb) ▪ DVD ROM ▪ SCSI/Fibre shared disk that supports the SCSI3 protocol ▪ Additional storage for PSM (optional) [2]	▪ 4X Eight core processors (Intel compatible) ▪ 64GB RAM ▪ Two 500GB SAS hot-swappable drives (15K RPM) ▪ RAID Controller ▪ 2X Network adapter (1Gb) ▪ DVD ROM ▪ SCSI/Fibre shared disk supports the SCSI3 protocol ▪ Additional storage for PSM (optional) [2]
Software prerequisites			
▪ Windows 2016 English Edition ▪ Windows 2012 R2 Standard Edition ▪ Windows 2012 R2 English/German versions [3] ▪ Windows 2008 R2 SP1 (64-bit) Enterprise Edition English/German version ▪ .NET Framework 4.5.2			

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)

Note:
Cluster Nodes must be installed only on physical servers.

PVWA and CPM servers

The following table lists the recommended specifications for the PVWA and CPM servers [1] .

Specifications

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
▪ Quad core processor (Intel compatible) ▪ 8GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 2X Quad core processor (Intel compatible) ▪ 16GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 2X Eight core processors (Intel compatible) ▪ 32GB RAM ▪ 2X 80GB SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 4X Eight core processors (Intel compatible) ▪ 64GB RAM ▪ 2X 80GB SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM
Software prerequisites [3]			
▪ Windows 2016, Windows 2012 R2 ▪ IIS 10.0, 8.5, 7.5 respectively ▪ .NET Framework 4.5.2 or 4.6.2 For Windows 2016, we recommend installing .Net Framework 4.7.1 with update KB4054856 ▪ Internet Explorer 11.0 or Chrome 56 and higher			

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
▪ PVWA and CPM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms			

PSM servers

The following table lists the recommended specifications for PSM servers.

Specifications

Small implementation (1-10 concurrent RDP/SSH sessions)	Mid-range implementation (11-50 concurrent RDP/SSH sessions)	Large implementation (51-100 concurrent RDP/SSH sessions)
Hardware Specifications: Physical Servers		
▪ 8 core processor (Intel compatible) ▪ 8GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 16 core processors (Intel compatible) ▪ 16GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 32 core processors (Intel compatible 2.1 GHz - 2.6 GHz) ▪ 32GB RAM ▪ 2X 250GB SAS hot-swappable drives (15K RPM) ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM
General Notes: . The concurrency of 100 sessions per PSM server should not be exceeded. . The concurrent sessions ranges are based on the RDP and SSH connections performance measurements. . Running resource-intensive applications like Toad, vSphere Client and so on, on the PSM server will result in lower concurrency. . The concurrent session's ranges assume the PSM is running on a dedicated server. . The concurrent session's ranges are based on performance measurements while video recording user's activities in HD resolution (one screen). Note that video recording resolution is affected by the desktop resolution of the client machine from which the connection was made. This means that performing connections from client machines with more than one HD screen, or with a higher resolution screen, will result in lower concurrency. **Server Virtualization Note:** . Installing the PSM server on a virtual machine requires allocating virtual hardware resources that are equivalent to the physical hardware specifications. For details, refer to the Recommended Settings For Installing PSM On a Virtual Machine chapter in the *Privileged Access Security Installation Guide.* . The maximum concurrency is lower (up to 40%) when installing the PSM server on a virtual machine.		
Software Prerequisites		
. Windows 2016, Windows 2012 R2 . Windows update KB2999226 . .NET Framework 4.5.2 - 4.7.1		

Small implementation (1-10 concurrent RDP/SSH sessions)	Mid-range implementation (11-50 concurrent RDP/SSH sessions)	Large implementation (51-100 concurrent RDP/SSH sessions)
. Microsoft Remote Desktop Services (RDS) Session Host . Microsoft Remote Desktop Services Gateway (optional) . PSM can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms		

PSMP servers

The following table lists the recommended specifications for PSMP servers.

Specifications

Small implementation (<100 concurrent sessions)	Mid-range implementation (100-200 concurrent sessions)	Large implementation (>200 concurrent sessions)
Hardware Specifications: Physical Servers		
▪ Quad core processor (Intel compatible) ▪ 8GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 2X Quad core processor (Intel compatible) ▪ 16GB RAM ▪ 2X 80GB SATA/SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM	▪ 2X Eight core processors (Intel compatible) ▪ 32GB RAM ▪ 2X 80GB SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM
Server Virtualization Note: Installing the PSMP server on a virtual machine requires allocating virtual hardware resources that are equivalent to the physical hardware specifications.		
Software Prerequisites		
▪ Red Hat Enterprise Linux 5.x versions (5.6 and above), 6.x versions (6.4 and above) and 7.x versions. ▪ CentOS Linux 5.x versions (5.6 and above), 6.x versions (6.4 and above) and 7.x versions.  **Note:** Security patches, and OS vendor recommended minor 5.x, 6.x or 7.x RHEL and CentOS upgrades can be applied on the server without reinstalling the PSMP		

Small implementation (<100 concurrent sessions)	Mid-range implementation (100-200 concurrent sessions)	Large implementation (>200 concurrent sessions)
▪ SUSE Linux Enterprise Server 11 SP4 or 12 ▪ PSM SSH Proxy can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platforms		

System Requirements by Product

The following system requirements list the most up-to-date supported platforms, including service packs. Unless otherwise specified, new service packs are not automatically supported.

CyberArk may choose not to provide maintenance and support services for the CyberArk Privileged Access Security (PAS) solution with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

In this section:

Digital Vault Server

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk Digital Vault Server with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum requirements

The Digital Vault server requires an Intel Pentium IV (or compatible) processor or higher.

To ensure maximum protection for the sensitive data inside the Digital Vault Server, the server is designed to be installed on a dedicated computer in a clean environment that does not have any additional software installed on it.

Supported platforms

The Digital Vault server is currently supported on the following platforms:

- Windows 2016 English Edition
- Windows 2012 R2 Standard Edition
- Windows 2012 R2 English/German Edition
- Windows 2008 R2 with Service Pack 1 (64-bit) English/German Edition

Software requirements

- .NET Framework 4.5.2

Supported LDAP directories

The Privileged Access Security solution provides standard LDAP v3 support and has been tested and certified with the following directories.

Directories:

Directory	Platforms
MS Active-Directory – Each of the following platforms is supported with its corresponding functional level:	. Windows 2008 . Windows 2012 . Windows 2012 R2 . Windows 2016
Sun One v5.2	
IBM Tivoli Directory Server v6.0	

Directory	Platforms
Novell eDirectory v8.7.1	
Oracle Internet Directory v10.1.4	

This list may be updated frequently as additional directories are certified. Please contact CyberArk Customer Support for information about additional directories that are not mentioned in the list above.

Supported ciphers for syslog servers

The following ciphers are supported for encrypted communication between the Vault and syslog servers:

ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES128-SHA
DHE-RSA-AES256-SHA
DHE-RSA-AES128-SHA256
DHE-RSA-AES256-SHA256

CyberArk component compatibility

Digital Vault server

CyberArk component	Compatible versions
PrivateArk Client/WebClient	8.0
Central Policy Manager	10.2
Password Vault Web Access	10.2
Privileged Session Manager	9.0.1 or higher
Privileged Session Manager SSH Proxy	7.2.9 or higher
On-Demand Privileges Manager	6.0 or higher
Credential Provider	4.5 or higher

Distributed Vaults compatibility

CyberArk clients on a Satellite Vault

Client	Compatible versions
Credential Provider	9.7
ExportVaultData utility	9.8 or higher
PAReplicate utility	9.8 or higher

All other clients can only run on a Master Vault.

High Availability

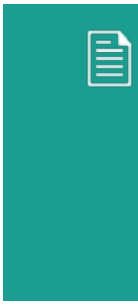
CyberArk High-Availability Digital Vault server for Windows 2008

The minimum requirements for the High-Availability Digital Vault server are as follows:

- Windows 2008 R2
  - Two Domain Controllers
  - DNS server
- Microsoft Cluster Service

CyberArk Digital Cluster Vault server for Windows 2012 R2 and Windows 2016

The minimum requirements for the CyberArk Digital Cluster Vault Server are as follows:

Requirement	Description
Windows 2012 R2 or Windows 2016 English Edition	 **Note:** In Windows 2012, if the CyberArk Digital Cluster Vault Server is being installed on an iSCSi network storage location over TCP/IP, Windows update KB2955164 must be installed to prevent data corruption.
Servers	Only physical servers are supported. You can install Vaults on Virtual machines using virtual availability solutions offered by the various vendors.
Both nodes must have the same amount of physical memory.	If the two nodes do not have the same amount of physical memory, update the innodb_log_file_size parameter in the my.ini file of the second node and specify the same value as in the first node.
Both nodes must be connected directly via a private network or cross-over cable.	This network must contain only the Vault Cluster machines in order to keep the Vault Cluster isolated and secure.
Shared storage that supports the SCSI3 protocol.	▪ CyberArk recommends using SAN with Fibre channel, which is faster and more reliable. ▪ Use GPT and MBR disks, not dynamic disks.

Requirement	Description
Quorum disk	Do not use Multipath I/O.
NIC configuration	You must use crossover cables for the private network. NIC teaming in load balancing mode is not allowed. Only an Active-Passive configuration is allowed. For details on configuring the NIC teaming, refer to https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/create-a-new-nic-team.
Each Vault Cluster server must have only one static IP, in the same subnet as the virtual IP.	
The clocks on both nodes must be synchronized.	

PrivateArk Client

The PrivateArk Client is the Windows interface for performing administrative operations in the Privileged Access Security solution, such as user management.

Note:
CyberArk may choose not to provide maintenance and support services for the PrivateArk Client with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum requirements

Platform:	Intel Pentium IV (or compatible) or higher
Disk space:	10MB free disk space
Minimum memory:	256MB
Communication:	TCP/IP connection to the Digital Vault server

Supported platforms

The PrivateArk Client is currently supported on the following platforms:

- Windows 2016 (If installed on the Vault server)
- Windows 2012 R2
- Windows 10
- Windows 2008 R2 with Service Pack 1 (64-bit)
- Windows 2008 (32-bit)
- Windows 7 with Service Pack 1 (32-bit and 64-bit)

Reports that are generated in the PrivateArk Client can either be saved to a text file, or to any of the following Office applications:

- Excel XP, Excel 2003, Excel 2007, Excel 2010

CyberArk component compatibility

The PrivateArk Client/WebClient v8.0 works with the Digital Vault Server, version 8.1 or higher.

NT Authentication Agent

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk NT Authentication Agent with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum requirements

- Windows 2012 R2
- Windows 2008 R2 with Service Pack 1
- Windows 2003 with Service Pack 2 (32-bit)

CyberArk Vault Backup Utility

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk Vault Backup Utility with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum requirements

- Windows 2012 R2
- Windows 2008 R2 with Service Pack 1 English Edition
- Windows 2003 with Service Pack 2 (32-bit)

Remote Control Client

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk Remote Control Client with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum requirements

- Windows 2012 R2
- Windows 2008 R2 with Service Pack 1
- Windows 2003 with Service Pack 2 (32-bit)
- Windows XP with Service Pack 3 (32-bit)

Central Policy Manager

Note:
CyberArk may choose not to provide maintenance and support services for the Central Policy Manager with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum system requirements

The Central Policy Manager (CPM) is a Privileged Access Security component and does not require a dedicated machine. However, it must be installed on a machine that is accessible to the network.

Minimum requirements

Platform:	Intel Pentium IV (or compatible) or higher
Disk space:	15MB free disk space for installation, and additional space for log files
Minimum memory:	4 GB
Communication:	TCP/IP connection to the Digital Vault Server
Software:	▪ Windows 2016 Windows 2012 R2 Windows 2008 R2 with Service Pack 1 ▪ Internet Explorer 8.0, 9.0, 10.0 and 11.0 ▪ .NET Framework 4.5.2

For specific system requirements of the different plug-ins of the Central Policy Manager, see the Privileged Access Security Implementation Guide.

CyberArk component compatibility

The Central Policy Manager works with the following CyberArk components:

Component	Compatible Versions
Digital Vault server	version 10.2
Password Vault Web Access	version 10.2
Privileged Session Manager	version 9.0.1 or higher
Privileged Session Manager SSH Proxy	versions 7.2.5 and higher
On-Demand Privileges Manager	versions 6.0 and higher
Credential Provider	version 4.5 or higher

Automatic password management

This section lists the platforms on which the CPM supports automatic password management and which are installed automatically with the CPM. For a complete list of supported devices, refer to the CPM Supported Devices document.

Operating Systems

Automatic password management is supported on the following platforms on IPv4 and IPv6:

Platform	Supported Versions
Windows Domain users	. Windows 2016 Active Directory domain . Windows 2012/2012 R2 Active Directory domain . Windows 2008/2008 R2 with Service Pack 1 Active Directory domain . Windows 2003 server
Windows Local users	. Windows 2016 server - only local administrators . Windows 2012/2012 R2 server . Windows 2008/2008 R2 server with Service Pack 1 . Windows 2003 server . Windows 10 . Windows 8 . Windows 7 with Service Pack 1 . Windows Vista
Windows Local users with WMI	. Windows 2016 server . Windows 2012/2012 R2 server . Windows 2008 server . Windows 2003 server . Windows 10 . Windows 8 . Windows 7 . Windows Vista
Windows Services	. Windows: . Windows 2016 server . Windows 2012/2012 R2 . Windows 2008/2008 R2 with Service Pack 1 . Windows 2003 . Windows 10 . Windows 8 . Windows 7 with Service Pack 1 . Windows Vista . Microsoft SQL Server 2005/2008 . Microsoft SQL Cluster Service 2005/2008
Windows Scheduled Tasks	. Windows 2016 server

Platform	Supported Versions
	. Windows 2012/2012R2 . Windows 2008/2008R2 with Service Pack 1 . Windows 2003 . Windows 10 . Windows 8 . Windows 7 with Service Pack 1 . Windows Vista **Note:** ▪ In order to manage Windows Scheduled Tasks on Windows 7, Windows 2008 Server, and Windows Vista, the CPM must be installed on Windows 2008 R2 with Service Pack 1 or 2012 server. ▪ In order to manage Windows Scheduled Tasks on Windows 10, the CPM must be installed on Windows 2012 server.
Windows IIS Application Pools	. Windows 2016 server . Windows 2012/2012 R2 . Windows 2008/2008 R2 with Service Pack 1 (with "IIS 6 management compatibility" role service) . Windows 2003
Windows IIS Directory Security (Anonymous Access)	. Windows 2016 server . Windows 2012/2012 R2 . Windows 2008/2008 R2 with Service Pack 1 . Windows 2003
COM+ Applications	. Windows 2016 server . Windows 2012/2012 R2 . Windows 2008/2008 R2 with Service Pack 1 . Windows 2003
Unix passwords	. Solaris Intel 9, 10, 11 . Solaris Sparc 10, 11 . Oracle Enterprise Linux 5 (32-bit and 64-bit) . HP-UX 11.x **Note:** Automatic password management is only supported on IPv4. . IBM AIX 5.3, 6.1, 7.1 . RHEL 4-7.1

Platform	Supported Versions
	 **Note:** For higher versions, additional customizations may be required. . Ubuntu 12.04 . Fedora 18, 22, 23 . CentOS 6 (32-bit and 64-bit) . SUSE Linux 10, 11, 12 . Cygwin
AS400 (iSeries) passwords	. AS400 (iSeries) computers using OS/400 V5R2 or higher  **Note:** Automatic password management is only supported on IPv4.
OS/390 (Z/OS) passwords	. OS/390 (Z/OS) machines for RACF users' passwords  **Note:** Automatic password management is only supported on IPv4.

Databases

Automatic password management is supported on the following platforms on IPv4 and IPv6:

Platform	Supported Components
Databases that support ODBC Connections	. All databases that support ODBC version 2.7 and higher  **Note:** For higher versions, additional customizations may be required.
Oracle Database passwords	. Oracle Database v8i-v12c . Oracle ODBC driver (can be installed as part of the Oracle Client installation V8i or higher)  **Note:** For higher versions, additional customizations may be required.

Platform	Supported Components
Microsoft SQL Server passwords	▪ Microsoft SQL Server 7, 2010, 2012, 2014, 2016  **Note:** For higher versions, additional customizations may be required.
Sybase database passwords	▪ Sybase Adaptive Server Enterprise 12.5.2, 16  **Note:** For higher versions, additional customizations may be required.
MySQL Server passwords	▪ MySQL version 5 - 5.7
DB2 passwords	▪ Windows platforms: ▪ IBM DB2 on Windows 2003, WinNT ▪ Unix platforms: ▪ IBM DB2 on the following Unix platforms: Red Hat Linux 8, Red Hat Enterprise Linux ES 3.0, Sun Solaris 5.8, IBM AIX 5, HP-UX 11.x  **Note:** For higher versions, additional customizations may be required.
Informix passwords	▪ Windows platforms: ▪ IBM Informix on Windows 2003, WinNT platforms ▪ Unix platforms: ▪ IBM Informix on the following Unix platforms: Red Hat Linux 8, Red Hat Enterprise Linux ES 3.0, Sun Solaris 5.8, IBM AIX 5, HP-UX 11.x  **Note:** For higher versions, additional customizations may be required.

Remote Access

Automatic password management is supported on the following platforms:

Platform	Supported Versions
HP iLO accounts:	iLO v2.0, 3.0 and 4.0
Dell DRAC passwords:	DRAC 5-8

Security Appliances

Platform	Supported Versions
CheckPoint Firewall-1 NG passwords:	CheckPoint Firewall-1
NetScreen Firewall passwords:	NetScreen version 5.3.or 2.0  **Note:** For higher versions, additional customizations may be required.
RSA Authentication Manager Accounts	RSA Authentication Manager 8.1, 8.2

Network Devices

Platform	Supported Versions
Cisco Router passwords:	Cisco Routers that support IOS 12.3 or higher through Telnet, for the following modes: . regular user . enable . terminal  **Note:** For higher versions, additional customizations may be required.
Cisco PIX passwords:	Cisco PIX machines, version 6.3 or higher, for the following modes: . enable . terminal  **Note:** For higher versions, additional customizations may be required.

Directories

Platform	Supported Versions
Novell eDirectory Passwords:	Novell eDirectory version 8.7.1 SMP or higher
SunOne Directory Passwords:	SunOne Directory Server version 5.2

Applications

Application	Supported Versions
Digital Vault passwords:	Digital Vault v4.0 or higher
SAP Application Server	

Cloud Services

- Amazon Web Services (AWS)
- Microsoft Azure

Others

- Passwords stored in Windows Registry

Password Vault Web Access

Note:
CyberArk may choose not to provide maintenance and support services for the Password Vault Web Access with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum system requirements

The Password Vault Web Access (PVWA) is a CyberArk component that enables you to access and configure the Privileged Access Security solution over the Web. The PVWA does not require a dedicated machine. However, it must be installed on a machine that is accessible to the network.

Minimum requirements

Platform:	Intel Pentium IV (or compatible) or higher
Disk space:	15MB free disk space for installation, and additional space for log files
Minimum memory:	2 GB
Communication:	TCP/IP connection to the CyberArk Password Vault Server
Software:	▪ Windows 2016 Windows 2012R2 Windows 2008R2 with Service Pack 1 Windows 2008R2 ▪ IIS 10.0 (Windows 2016) IIS 8.5 (Windows 2012 R2) IIS 7.5 (Windows 2008 R2/Windows 2008 R2 SP1) ▪ Internet Explorer 11.0 ▪ .NET Framework 4.5.2 or 4.6.2 For Windows 2016, we recommend installing .Net Framework 4.7.1 with update KB4054856

Supported browsers

PVWA v10 interface

The PVWA interface for version 10.2 is supported on the following browsers:

- Chrome 56 and higher
- Internet Explorer 11.0 on Windows

- **Prerequisites:**
  - In **Internet Options → Security Settings → Downloads** and select the following:
    - File download → Enable
    - Font download → Enable

PVWA Classic interface

The PVWA interface for version 9 is supported on the following browsers:

- Internet Explorer 8.0, 9.0, 10.0 and 11.0 on Windows

Note:
- For IE 9.0, the PVWA requires IE 8 compatibility mode.
- For IE 10.0, install hotfix KB2836943 on the PVWA server.

- Chrome: Any version released in the last six months
- Firefox: Any version released in the last six months on Windows and Linux/UNIX

Note:
- Make sure that Firefox includes the Java plug-in.

Supported connections

- PSM connections to remote machines are supported with IPv4 and IPv6 addresses.

Supported Ticketing Systems

The following ticketing systems are supported out-of-the-box:

- ServiceNow Geneva, Helsinki, Istanbul, and Kingston
- BMC Remedy v9.1

For details about configuring other ticketing systems, see the Privileged Access Security Implementation Guide .

Requirements on end-user machines

Required Component	Version
RDP ActiveX Client	5.2 or higher for environments set up to use an ActiveX connection method for PSM connection)
CyberArk PSM codec	For viewing high compression session recordings with an external player (e.g. Windows Media Player). The **PSMCodec.exe** is included in the PSM installation package and is required to enable users to view PSM recordings with a regular media player (not PSM Direct Playback).
JRE (Java Runtime Environment)	JRE 1.4, or higher (for SSH transparent connections)

Required Component	Version
Adobe Flash player	10.0 browser add-on, or higher (for PSM Direct Playback with IE browser) **Note:** ▪ For PSM Connections make sure that your CyberArk license includes the relevant a license for an external tool that will support these connections. ▪ Currently this external tool doesn't support connections when RD Gateway is configured in the environment. For more information, refer to Configuring PSM Connections in the Privileged Access Security Implementation Guide.

Supported mobile devices

The following mobile devices support the v9 Mobile PVWA on the Privileged Access Security solution:

- iPhone Smartphones
- Blackberry Smartphones
- Android-powered Smartphones

Supported languages

The PVWA supports the following languages:

PVWA v10 interface

- English

PVWA Classic interface

- English
- French
- Spanish
- German
- Russian
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese
- Brazilian Portuguese

CyberArk component compatibility

The PVWA works with the following CyberArk components:

Component	Version
Digital Vault Server	10.2
Central Policy Manager	10.2

Component	Version
Privileged Session Manager	9.0.1 or higher
Privileged Session Manager SSH Proxy	7.2.9 or higher
On-Demand Privileges Manager	6.0 or higher
Credential Provider	4.5 or higher

Accounts Feed

Scan for Windows accounts

Discovery processes detect the following Windows accounts:

- Local accounts
- Domain accounts

Discovery processes detect the following dependencies:

- Windows Services accounts
- Scheduled Tasks accounts
- IIS Application Pools accounts
- IIS Directory Security (Anonymous Access) accounts
- COM+ Applications accounts

Note:
When scanning a specified domain, the discovery automatically retrieves information about discovered accounts that is stored in trusted domains, without requiring additional permission. Specifically, the discovery only retrieves information about Windows Services dependencies and Scheduled Tasks dependencies that derive from trusted domains.

Supported Active Directory

- Microsoft Active Directory 2008, 2012 and 2016

Note:
The Discovery does not support scanning Active Directory domain controllers

Credentials for scanning

Credentials for scanning

Scanning Location	Required Credentials
Active Directory	Read permissions in the OU to scan and all sub-OUs
Target machines	Domain Administrator, or

Scanning Location	Required Credentials
	Equivalent Domain User: ▪ User with read permissions on the Active Directory ▪ User with local administrative rights for Windows on the target machine ▪ User with permissions to logon remotely to the target machine **Note:** In Windows Vista or newer, the domain user must belong to the Administrators group or to a group nested within the Administrators group. In older versions of Windows, the domain user can be a member of any privileged group

Supported target computers

Supported workstations

- Windows Vista
- Windows 7
- Windows 8
- Windows 10

Supported servers

- Windows 2003
- Windows 2008
- Windows 2012
- Windows 2016

Supported target computers for discovering dependencies

Supported servers:

- Windows 2003
- Windows 2008/2008R2 with Service Pack 1
- Windows 2012/2012R2
- Windows 2016

Note:
- To discover Scheduled Tasks on Windows 2012, the CyberArk Scanner (CPM) must be installed on Windows 2012.

- To discover IIS Application Pools accounts, IIS Directory Security (Anonymous Access) accounts and COM+ Applications accounts, IIS7.5 or 8.5 must be installed.

Supported protocols

Protocols that are supported when accessing the Active Directory

- LDAPS (default)

Note:
To support LDAPS in discoveries, this protocol must be configured in the Active Directory

- LDAP

Network protocols

- Windows File and Print Sharing
- Windows (WMI)

For details about how to enable the Windows (WMI) Protocol in your environment, see *Appendix G: Enabling WMI Ports on Windows Client Machines* in the *Privileged Access Security Implementation Guide.*

For more information about the ports that EPV uses to access remote machines, refer to Standard Ports used for Accounts Discovery, page 86.

Scan for Unix accounts

Discovery processes detect the following Unix accounts:

- Local accounts

Note:
Domain users that are used to authenticating to Unix machines (using AD Bridge integration) are currently not discovered

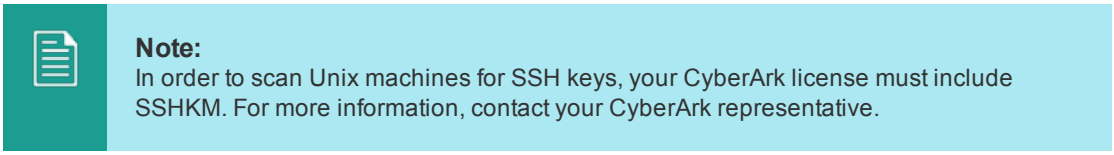
- SSH Keys and their trusts

Credentials for Scanning Local Accounts

At least one of the following privileges

Privilege	Enables user to retrieve …
root or user with uid=0	All account details
sudoers for the "cat /etc/passwd" command	The minimum details required to create a pending account (user name and address)
sudoers for the following commands: ▪ cat "/etc/shadow" ▪ cat "/etc/passwd" ▪ cat "/etc/security/passwd" (AIX) ▪ cat "/etc/security/lastlog" (AIX) ▪ cat /etc/group ▪ cat "/etc/sudoers" ▪ lastlog | grep -v '*' ▪ hostname –s ▪ ls -d /etc/[A-Za-z]*[_-][rv]e [lr]* | grep v 'lsb|os|system' ▪ test -f "{0}"; echo $?	All account details

Credentials for scanning SSH Keys



Note:
In order to scan Unix machines for SSH keys, your CyberArk license must include SSHKM. For more information, contact your CyberArk representative.

At least one of the following privileges

Privilege	Enables user to retrieve …
user with uid=0	All account details
sudoers for the "cat /etc/passwd" command	The minimum details required to create a pending account (user name and address)
sudoers for the following commands: ▪ **Linux:** uname, ls, test, cat, lastlog, getent, grep, wc, find, xargs, ssh-keygen, echo, rm, date, hostname, ifconfig ▪ **AIX:** uname, ls, test, cat, lsdev, grep, wc, ssh-keygen, echo, rm, istat, hostname, ifconfig ▪ **Solaris:** uname, echo, test, cat, getent, grep,	All account details

Privilege	Enables user to retrieve …
▪ psrinfo, wc, find, xargs, ssh-keygen, ls, rm, truss, hostname, ifconfig All account details	

Supported Unix platforms

- RHEL 4-7.1
- Solaris Intel and Solaris SPARC 9, 10, 11
- AIX 5.3, 6.1, 7.1
- ESXi 5.0, 5.1
- SUSE 10
- Fedora 18,19, 20
- CentOS 6
- Oracle Linux 5

Supported Sudo replacements solutions

- CA Privileged Identity Manager/ControlMinder – This solution contains the sesudo command.
- Centrify Access Manager/DirectAudit - This solution contains the dzdo command.

Enable the Windows (WMI) protocol in your environment

Enable WMI protocol

1. Make sure the Windows Management Instrumentation service startup type is set to Automatic.
2. For your operating system, do the following:
   - **Windows 7** - In the firewall settings for your local or Group policy, under **Inbound Rules**, make sure **Windows Management Instrumentation (WMI-In)** is enabled and allowed for the Domain profile.
   - **Windows Vista** - In the firewall settings for your local or Group policy, click the **Exceptions** tab and enable the **Windows Management Instrumentation (WMI)** exception.

SSH Key Manager

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk SSH Key Manager with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

The SSH Key Manager (SSHKM) supports SSH Keys lifecycle management and helps organizations eliminate risks that are inherent in using SSH Keys. In addition, it enables organizations to meet their audit requirements by simplifying and automating SSH Keys management. The SSH Key Manager is built on top of the Privileged Account shared Platform Technology and benefits from the suite infrastructure, including the Digital Vault, Master Policy, integrations and more. The SSH Key Manager doesn't have a dedicated component to install; it requires the installation of the CPM and PVWA and a relevant license.

CyberArk component compatibility

The SSHKM is compatible with the following CyberArk components:

Component	Compatible Version
Digital Vault server	version 9.10 or higher
Central Policy Manager	version 9.9.5 or higher
Password Vault Web Access	version 9.10 or higher
Privileged Session Manager	version 9.0.1 or higher
Privileged Session Manager SSH Proxy	versions 7.2.5 or higher
On-Demand Privileges Manager	versions 6.0 or higher
Credential Provider	version 4.5 or higher

Automatic SSH key rotation

The SSH Key Manager (SSHKM) supports automatic management of SSH Keys and their trusts on the following Unix platforms. For a complete list of supported devices, refer to the Supported Devices document.

Operating systems

Operating System	Compatible Versions
RHEL	4-7.1
AIX	5.3, 6.1, 7.1
Solaris Intel and Solaris SPARC	9, 10, 11
ESXi	5.0, 5.1, 6.0, 6.5
SUSE	10
Fedora	18,19, 20, 24, 26
CentOS	6
Oracle Linux	5
HP-UX	11.x

Credentials for scanning SSH keys

To scan SSH keys and their trusts, the user performing the scan requires at least one of the following privileges:

Privilege	Enables user to retrieve …
user with uid=0	All account details
sudoers for the "cat /etc/passwd" command	The minimum details required to create a pending account (user name and address)
sudoers for the following commands:Linux: uname, ls, test, cat, lastlog, getent, grep, wc, find, xargs, ssh-keygen, echo, rm, date, hostname, ifconfigAIX: uname, ls, test, cat, lsdev, grep, wc, ssh-keygen, echo, rm, istat, hostname, ifconfigSolaris: uname, echo, test, cat, getent, grep, psrinfo, wc, find, xargs, ssh-keygen, ls, rm, truss, hostname, ifconfig	All account details

Managing local copies of private SSH keys

The SSHKM manages local copies of private SSH Keys on the following platforms, in addition to all the platforms listed above:

- Fedora 18-23 (32 and 64-bit)
- SUSE 12 (64-bit)

Privileged Session Manager®

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk Privileged Session Manager® with relation to any end-user client machine or target platforms which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

The Privileged Session Manager® (PSM) is a CyberArk component that enables you to initiate, monitor and record privileged sessions and usage of administrative and privileged accounts. The PSM does not require a dedicated machine. However, it must be installed on a machine that is accessible to the network.

Note:
To achieve optimal concurrency it is recommended to install PSM on a dedicated machine.

Minimum system requirements

The minimum requirements for the PSM are as follows:

Platform:	Intel Pentium IV (or compatible) or higher
Disk space:	20GB free disk space for installation, and additional 20GB space for temporary workspace
Minimum memory:	8 GB
Communication:	TCP/IP connection to the Digital Vault Server
Software:	▪ Windows 2016 Windows 2012R2 ▪ .NET Framework 4.5.2 - 4.7.1 ▪ Remote Desktop Services (RDS) Session Host

Note:
Make sure you have the required number of RDS CALs to enable you to access the RDS server. For more information, refer to Connecting to the PSM server with Microsoft Remote Desktop Services (RDS) Session Host in the Privileged Access Security Installation Guide.

▪ Remote Desktop Gateway (optional)

- Before installing the PSM, make sure that the Users group has the Allow Logon Locally Windows permission in the local security policy. This ensures that the PSMShadowUsers group created during PSM installation will have the required permissions. Alternatively, you can set this local security policy permission for the PSMShadowUsers group directly after PSM installation.

PSM supported connections

The PSM supports connections to remote machines using IPv4 and IPv6 addresses with the following platforms out-of-the-box. Additional platforms can be supported and monitored using the PSM Universal Connector. For more information, refer to the Privileged Access Security Implementation Guide.

Platform	Additional Information
Unix, Linux and Network or any SSH-based devices	Support using the following protocols: ▪ SSH (including file-transfer capabilities) ▪ Telnet
Windows RDP (including file-transfer capabilities)	**Note:** Connections to and from Windows XP and prior Windows versions are not supported.
Windows Remotely Anywhere	
Windows RAdmin sessions	PSM can monitor remote administration through the RAdmin Tool. To monitor RAdmin sessions, install the following software on the PSM machine: ▪ RAdmin Viewer v3.4
AS400 (iSeries)	
OS/390 (Z/OS)	
Web-based interfaces, client, and custom applications	
PSM for Databases	PSM can monitor Oracle DBA sessions through the following DBA tools: ▪ Toad ▪ SQL*Plus To monitor Oracle DBA sessions, install the following software on the PSM machine: ▪ Toad for Oracle Base Edition v10.5.1.3 , v10.6.1.3 and v12.10(32 bit) ▪ Toad Admin Module v10.5.1.3 and 10.6.1.3 PSM can monitor Microsoft SQL Server DBA sessions through the following DBA tools:

Platform	Additional Information
	▪ SQL Server Management Studio 2008,2012, 2016, and 2017
PSM for Virtualization	PSM can monitor VMWare administration session through the following tools: ▪ vSphere Client to connect to vSphere / ESX hosts ▪ vSphere Client to connect to vCenter To monitor VMWare administrator sessions, install the following software on the PSM machine: ▪ vSphere Client v4.0, v4.1, v5.0, and v6.0

Storage requirement for PSM recordings

The Privileged Session Manager stores the session recordings on the Digital Vault server or an external storage device. The estimated storage requirement is approximately 50-250 KB for each minute of a recording session.

The recording size is affected by the type of the session recording (console vs. GUI recording) as well as by the type and number of activities that are performed during the session.

For example, 250GB of storage will be sufficient for recording 10 hours of activities per day retained for 5 years.

CyberArk component compatibility

The PSM is compatible with the following CyberArk components:

Component	Compatible Versions
Digital Vault server	versions 7.2.7 and higher
Password Vault Web Access	versions 7.2.7 and higher
Privileged Session Manager SSH Proxy	versions 7.2.9 and higher
CPM	Any CPM that is compatible with the above Digital Vault server and Password Vault Web Access. For more information, refer to CyberArk Component Compatibility for those components.

HTML5 Gateway

- A Web server, such as Tomcat, that can support Java 1.6 or above

Note:
The PSM Gateway supports Tomcat v 7 or above

- Hardware specifications

Small + Mid-range implementation (1-50 concurrent RDP/SSH sessions)	Mid-range + Large implementation (51-100 concurrent RDP/SSH sessions)	Very large implementation (101-200 concurrent RDP/SSH sessions)
▪ 2 core processors (Intel compatible) ▪ 4 GB RAM	▪ 4 core processors (Intel compatible) ▪ 8 GB RAM	▪ 8 core processors (Intel compatible) ▪ 16GB RAM

Note:
- Tests are based on 40% SSH and 60% RDP concurrent sessions running with ful HD resolution.
- These requirements are based on a dedicated machine for HTML5 Gateway.

Privileged Session Manager SSH Proxy

Note:
CyberArk may choose not to provide maintenance and support services for the CyberArk Privileged Session Manager SSH Proxy with relation to any end-user client machine or target platforms which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

The Privileged Session Manager SSH Proxy (PSMP) is a CyberArk component that enables you to secure, control and monitor privileged access to Linux and Unix systems, network devices and any other SSH-based devices. The PSMP requires a dedicated machine which is accessible to the network.

Minimum system requirements

The minimum requirements for the PSMP are as follows:

Platform:	Intel Pentium IV (or compatible) or higher
Disk space:	20GB free disk space for installation, and additional 20GB space for temporary workspace
Minimum memory:	2 GB
Communication:	TCP/IP connection to the Digital Vault Server
Operating System:	▪ Red Hat Enterprise Linux 6.x versions (6.4 and above) and 7.x versions. ▪ CentOS Linux 6.x versions (6.4 and above) and 7.x versions. **Note:** Security patches, and OS vendor recommended minor 6.x or 7.x RHEL and CentOS upgrades can be applied on the server without reinstalling the PSMP. ▪ SUSE Linux Enterprise Server 11 SP4 or 12

PSMP supported protocols

- Unix, Linux and Network devices using the following protocols:
  - SSH (including SSH-Tunneling)
  - Telnet

Supported SSH clients on the end-user machine

- The PSM SSH Proxy allows access from any SSH client that can connect to an OpenSSH 7.7 server.

Note:
OpenSSH 7.7 requires that Open SSL V1.01 or above be installed.

Supported connections

- The PSMP supports connections to remote machines using IPv4 and IPv6 addresses.

Storage requirement on the Digital Vault server

The PSMP stores the session recordings on the Digital Vault server. The estimated storage requirement is approximately 1-5 KB for each minute of a recording session. The recording size is affected by the number of activities that are performed during the session.

For example, 5 GB of storage will be sufficient for recording 10 hours of activities per day retained for 5 years.

CyberArk component compatibility

The PSM SSH Proxy is compatible with the following CyberArk components:

Component	Supported Versions
Digital Vault Server	Version 7.2.7 and higher
Password Vault Web Access	Versions 7.2.7 and higher
Privileged Session Manager	Versions 7.2.7 and higher
CPM	Any CPM that is compatible with the above Digital Vault server and Password Vault Web Access.

AD Bridge capabilities

AD Bridge connections are supported on the following platforms:

Platform	Supported Versions
AIX	5.3, 6.1, 7.1
CentOS	6.4
Fedora	18
RHEL	4, 5, 6, 7
Solaris Intel	5.9 ,5.10, 5.11
Solaris Sparc	5.9 ,5.10, 5.11
SUSE	10.x, 11.x, 12.x, 13.x
HP-UX	11.x
Debian	8.2
Ubuntu	14.04

The following CyberArk component versions are required:

Component	Required Versions
Digital Vault Server	Version 9.1 and higher
Password Vault Web Access	Versions 9.1 and higher
Privileged Session Manager	Versions 9.1 and higher

Privileged Threat Analytics

PTA Server System Requirements

You will receive the PTA installation package from your CyberArk support representative. It can be installed on the following platforms:

- VMWare Player 6.x and above
- VMWare Workstation 10.x and above
- VMWare ESX/i 5.5 and above
- Microsoft Hyper-V

Note:
Microsoft Hyper-V can be installed on Windows Server 2008R2, Windows Server 2012R2, or Windows Server 2016.

The PTA image must be installed on a dedicated machine that has access to the Vault, or to the primary Vault in a distributed Vault environment, and also to either the organizational SIEM solution, or UNIX inspected machines for syslogs.

The minimum requirements for installing this image on a VM machine are as follows:

- 8 Core-CPU
- 16 GB RAM memory
- 500 GB hard disk storage

Supported Browsers

PTA currently supports the following browsers:

- Internet Explorer 11.0
- Chrome - latest version
- Firefox - latest version

IP Requirements

PTA requires an IP in one of the following forms:

- **Static Address:** A static IP address.
- **DHCP:** If the organization has a DHCP server which dynamically allocates IP addresses, verify with the organization's IT that the PTA machine's IP address is locked.

DNS Requirements

- **DNS:** A DNS address record that maps the host name **PTAServer** to the IP address of the PTA machine. The DNS configured in PTA must recognize all the machines from which PTA will receive syslog messages. PTA requires both the Forward (A record) and Reverse (PTR record) lookup.

Domain Requirements (for Golden Ticket Detection only)

- PTA supports detection of Golden Ticket attacks for domains.
- The domains should be on Windows Server 2008 and above, with Function level 2003 and above.
- This applies both to domains and sub-domains.

LDAP/S Requirements

LDAP: PTA can integrate with LDAP to:

- Enable LDAP authentication
- Broaden and increase the accuracy of PTA detections

In order to integrate PTA with LDAP, define a group name in PTA which has the same name as the group **sAMAccountName**, which appears in Active Directory.

Note:
- To integrate with LDAP over SSL, create a dedicated security Base-64 encoded X.509 certificate.
- LDAP login and query permission are required for the bind user.
- Currently, PTA only integrates with Microsoft Active Directory LDAP.

Certificate Requirements

It is highly recommended that you use your organization's SSL certificate. Otherwise, you can use the self-signed certificate created during PTA installation.

If you use your organization's SSL certificate:

- The Certificate Signing Request (CSR) requires a Base-64 encoded X.509 SSL certificate.
- The SSL Certificate Chain requires a Base-64 encoded X.509 SSL certificate
- The SSL Certificate Issuer Chain requires a Base-64 encoded X.509 SSL certificate

CyberArk Vault / PAS Compatibility

Note:
This section is only applicable for users of PTA 10.3 and higher who are working with PAS 10.2 or lower.

Integration	Required Version
Integrate the Vault with **SIEM** and **PTA**	CyberArk Vault version **7.2.5** or higher
Support automatic threat containment using PAS integration, for **Overpass the Hash** attack and **Suspected Credential Theft** security events	CyberArk Vault version **9.3** or higher
Support **automatically adding unmanaged privileged accounts to the pending accounts queue**	CyberArk Vault version **9.7** or higher

Integration	Required Version
Configure **Golden Ticket detection**	CyberArk Vault version **9.8** or higher
Support the Privileged Session Management integration	CyberArk Vault and PVWA version **9.8** or higher **Note:** Privileged Session Management integration works with lower versions of CyberArk Vault, but without the ability to report Privileged Session Analysis results to PVWA.
Support a distributed Vault environment	CyberArk Vault version **9.9.5** or higher
Support sending PTA alerts to the Vault	CyberArk Vault version **9.10** or higher
Support the reconcile password for Suspicious Password Change	CyberArk Vault version **9.10** or higher
Support automatic session termination	CyberArk Privileged Access Security suite version **10.1** or higher

Supported Input Data Formats

Following are general guidelines for the data sent to PTA:

- PTA supports UTF-8 formatted data.
- **Windows**: The integration with Windows is based on authentication events 4624, 4723, and 4724. PTA supports these event types, which is supported in Windows 2003 and higher.

Note:
In order for PTA to monitor activity of privileged accounts in Windows machines, Windows security events 4624, 4723, and 4724 from each monitored Windows machine must be forwarded to the SIEM and from the SIEM to PTA.

- **Unix**: When collecting syslogs directly from Unix machines, PAM Unix is supported. PAM Unix is supported by multiple Unix flavors, such as Red Hat Linux, HP-UX, and Solaris.

  Supported PAM Unix events include accepted public key, accepted password, and session open.
- **Database**: Oracle logon events are supported.
- **Network Sensor**: Traffic is received from domain controllers in the environment.
- **Vault**: Specific events are accepted. Supported device types are operating system and database. You can also install a generic plugin to monitor additional accounts for additional platforms. For details, see the *Privileged Access Security Implementation Guide*.
- **Applications**: Successful logon events are accepted when you install a generic plugin. For details, see the *Privileged Access Security Implementation Guide*.

PTA Port Usage

Use the following tables as guidelines for PTA port usage.

- PTA Port Redirection Rules, page 50
- PTA Port Usage: Incoming Fixed Ports, page 50
- PTA Port Usage: Incoming Optional Ports, page 51
- PTA Port Usage: Outgoing Fixed Ports, page 51
- PTA Port Usage: Outgoing Optional Ports, page 52

Note:
All blocked communication is logged to **/var/log/iptables.log**.

PTA Port Redirection Rules

Use the following table for the PTA port re-directional rules.

#	Protocol	Source Port	Destination Port	Description
1.	TCP	80	8080	Redirect HTTP/S default ports to the Tomcat Web Server web ports
2.	TCP	443	8443	

PTA Port Usage: Incoming Fixed Ports

The port numbers in the following table are **fixed** and **cannot be changed**.

#	Protocol	Port	Description
1.	TCP	80	Allow incoming HTTP communication for the PTA web
2.	TCP	8080	This is redirected to HTTPS by the Tomcat Web Server
3.	TCP	443	Allow incoming HTTPS communication for the PTA web
4.	TCP	8443	

#	Protocol	Port	Description
5.	TCP	22	Allow remote access to the machine (SSH), for both secure telnet and SFTP
6.	UDP	67,68	Allow incoming data from the DHCP server
7.	ICMP	Echo Request	Allow standard ICMP pings to this server **Note:** Only echo-request is allowed
8.	-	-	Allow all local traffic within the server
9.	-	-	Allow replying to an already established session
10.	-	-	**All other communication is logged and rejected / dropped**

PTA Port Usage: Incoming Optional Ports

The port numbers in the following table can be changed to different port numbers according to the customer's environment.

#	Protocol	Port	Description
1.	TCP	514, 11514	Allow incoming syslog messages (could be configured for authorized sources only for specific IP addresses)
2.	UDP	514, 11514	
3.	TCP	6514, 7514	Allow incoming secure syslog messages for the PTA Windows Agent connection

PTA Port Usage: Outgoing Fixed Ports

The port numbers in the following table are **fixed** and **cannot be changed**.

#	Protocol	Port	Description
1.	TCP	514	Allow sending syslog messages in port 514
2.	UDP	514	
	TCP	80	Allow an outgoing HTTP connection to CyberArk PVWA for a specific IP address
	TCP	443	Allow an outgoing HTTPS connection to CyberArk PVWA for a specific IP address
3.	ICMP	Echo Request	Allow standard ICMP pings from this server **Note:** Only echo-request is allowed

#	Protocol	Port	Description
4.	UDP	53	Allow outgoing DNS requests
5.	UDP	123	Allow outgoing NTP requests
6.	-	-	Allow all local traffic within the server
7.	TCP/UDP	Broadcast	Allow broadcast (255.255.255.255) for outgoing DHCP requests
8.	-	-	Allow replying to an already established session
9.	-	-	**All other communication is logged and rejected / dropped**

PTA Port Usage: Outgoing Optional Ports

The port numbers in the following table can be changed to different port numbers according to the customer's environment.

#	Protocol	Port	Description
1.	TCP	25	Allow sending SMTP (email) messages for specific IP address
2.	TCP	587	
3.	TCP	3268, 389	LDAP for specific IP address
4.	TCP	3269, 636	LDAPS for specific IP address
5.	TCP/UDP	1858	Allow outgoing connection to the CyberArk Vault for specific IP address
6.	TCP/UDP	<port>	Outbound connection (SIEM integration) for specific port and IP address

PTA Windows Agents System Requirements

- Server authentication requires that a third-party certificate or your company's certificate is installed on your PTA Server machine.

Note:
Create a dedicated Base-64 encoded X.509 SSL certificate.

- Client authentication requires a SHA-256 certificate issued for the Domain Controller with the **Microsoft Enhanced RSA and AES Cryptographic Provider** CSP enabled for the Template. This CSP is disabled by default.

Note:
Create a dedicated Base-64 encoded X.509 SSL certificate.

- PTA Windows Agent works with the following Windows servers:

- Windows 2008 R2 64-bit
- Windows 2012 R2 64-bit
- Windows 2016 64-bit

PTA Network Sensors System Requirements

The PTA Network Sensor software can be installed on the following:

Hardware	See Reference
Physical server:	Refer to one of the following requirements lists: . PTA Network Sensor: Physical Hardware Requirements: Standard Configuration (Recommended), page 53 . PTA Network Sensor: Physical Hardware Requirements: Lighter Configurations, page 54
VM:	Support **VMware ESXi version 5.5 and higher**, hardware **version 8 and higher**.
	Refer to one of the following requirements lists: . PTA Network Sensor: VM Requirements: Standard Configuration (Recommended), page 54 . PTA Network Sensor: VM Requirements: Lighter Configurations, page 55

PTA Network Sensor: Physical Hardware Requirements: Standard Configuration (Recommended)

PTA Network Sensor software requires the following:

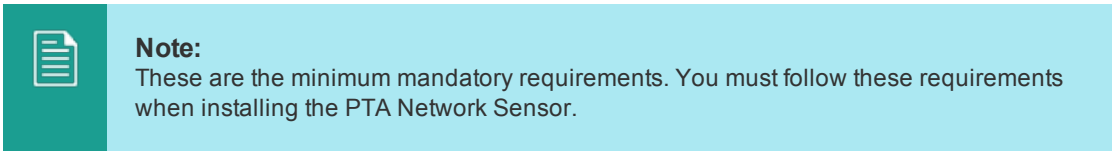
Note:
These are the minimum mandatory requirements. You must follow these requirements when installing the PTA Network Sensor.

Physical Hardware	Requirement
OS	CentOS 7.2 64-bit "minimal installation" build 1611
RAM	8GB
CPU	8 cores
Hard Disk Storage	250GB (SSD is recommended).
Management NIC	A NIC with a static IP address.
Traffic Monitoring NIC	The physical or virtual network interface that listens to the network traffic.

Physical Hardware	Requirement
NICs	In order to optimize the PTA Network Sensor performance, it is recommended to install an Intel NIC with one of the following chipsets: . 82540, 82545, 82546 . 82571..82574, 82583, ICH8..ICH10, PCH..PCH2 . 82575..82576, 82580, I210, I211, I350, I354, DH89xx . 82598..82599, X540, X550 . X710, XL710

PTA Network Sensor: Physical Hardware Requirements: Lighter Configurations

In lighter environments, PTA Network Sensor software requires the following:



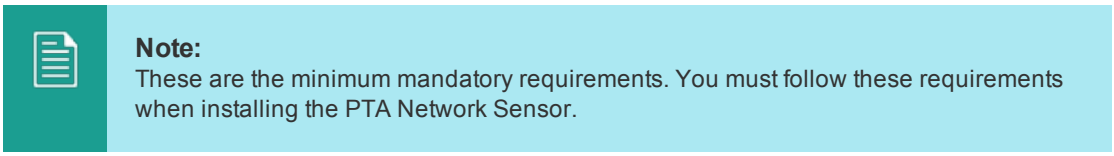
Note:
These are the minimum mandatory requirements. You must follow these requirements when installing the PTA Network Sensor.

Physical Hardware	Requirement
OS	CentOS 7.2 64-bit "minimal installation" build 1611
RAM	4GB
CPU	4 cores
Hard Disk Storage	80GB (SSD is recommended).
Management NIC	A NIC with a static IP address.
Traffic Monitoring NIC	The physical or virtual network interface that listens to the network traffic.
NICs	In order to optimize the PTA Network Sensor performance, it is recommended to install an Intel NIC with one of the following chipsets: . 82540, 82545, 82546 . 82571..82574, 82583, ICH8..ICH10, PCH..PCH2 . 82575..82576, 82580, I210, I211, I350, I354, DH89xx . 82598..82599, X540, X550 . X710, XL710

PTA Network Sensor: VM Requirements: Standard Configuration (Recommended)

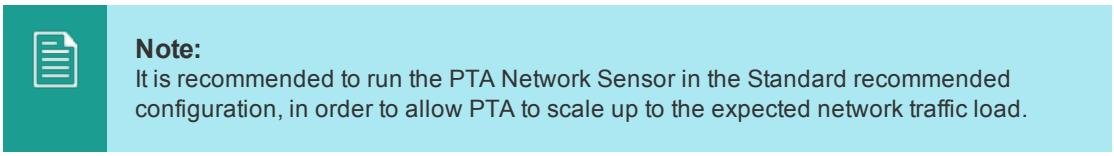
IMPORTANT: Only the below configurations are supported!

PTA Network Sensor software requires the following VM requirements:



Note:
These are the minimum mandatory requirements. You must follow these requirements when installing the PTA Network Sensor.

Virtual Machine	Requirement
RAM	8GB
CPU	8 cores
Hard Disk Storage	40GB (SSD is recommended).
VM	. Use the ESXi setup to define the PTA Network Sensor VM as High Priority. . Configure promiscuous mode or port mirroring on the ESXi server.
VM Network Driver	VMXNET3
NICs	Any NIC

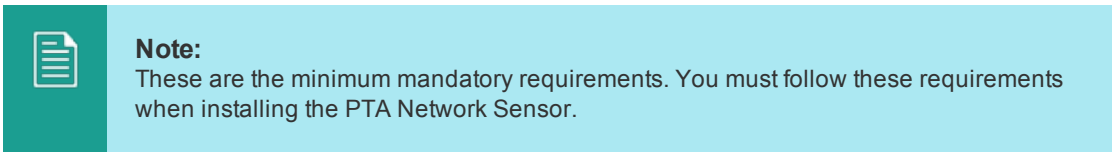


Note:
It is recommended to run the PTA Network Sensor in the Standard recommended configuration, in order to allow PTA to scale up to the expected network traffic load.

PTA Network Sensor: VM Requirements: Lighter Configurations

IMPORTANT: Only the below configurations are supported!

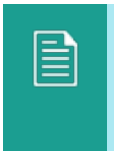
In lighter environments, PTA Network Sensor software requires the following VM requirements:



Note:
These are the minimum mandatory requirements. You must follow these requirements when installing the PTA Network Sensor.

Virtual Machine	Requirement
RAM	4 GB
CPU	4 cores
Hard Disk Storage	40 GB (SSD is recommended).
VM	. Use the ESXi setup to define the PTA Network Sensor VM as

Virtual Machine	Requirement
	High Priority. . Configure promiscuous mode or port mirroring on the ESXi server.
VM Network Driver	VMXNET3
NICs	Any NIC



Note:
It is recommended to run the PTA Network Sensor in the Standard recommended configuration, in order to allow PTA to scale up to the expected network traffic load.

Application Identity Management

Note:
CyberArk may choose not to provide maintenance and support services for CyberArk's Application Identity Management with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Credential Provider

The Credential Provider enables controlled and constant access to credentials stored in the Vault, eliminating the usage of embedded and hard coded privileged credentials in applications, scripts and services.

Supported platforms

The Credential Provider is currently supported on the following platforms:

Platform	Latest Version
AIX	9.9.5
Solaris Intel	9.9.5
Solaris UltraSparc	9.9.5
Linux Intel	9.9.5
Linux On PowerPC	9.9.5
Windows	9.9.5
zLinux	6.0
HP-UX[1]	4.5

[1]The Credential Provider on HP-UX is currently released as controlled availability only as v4.5. For more information, contact your CyberArk representative.

Credential Provider on AIX (v9.9.5)

The Credential Provider for AIX is supported on the following platforms:

- AIX 6.1, and 7.1 TL1, TL2, and TL3 (64-bit)

Credential Provider on Solaris (v9.9.5)

The Credential Provider for Solaris is supported on the following platforms:

Platform	Supported Versions
Solaris Intel 11	SunOS 5.11
Solaris Intel 10	SunOS 5.10 64-bit
Solaris SPARC 10,11 64-bit	SunOS versions 5.10 and 5.11 64-bit

Credential Provider on Linux (v9.9.5)

The Credential Provider for Linux is supported on the following platforms:

Platform	Supported Versions
RHEL	Intel 5, 6 and 7 (32/64-bit)
RHEL	Power PC 7.1(Little Endian) 64-bit
SUSE	Intel 10, 11 and 12 (64-bit)
SUSE	Intel 11 and 12(64-bit)
CentOS	Intel 5, 6 and 7 (32/64-bit)
Fedora	13 and 14 (32-bit)

Credential Provider on Linux (v7.20.110)

The Credential Provider for Linux is supported on the following platforms:

Platform	Supported Versions
Ubuntu	12.04 LTS 64-bit
Platform	Supported Versions

Credential Provider on Docker (1.11)

The Credential Provider is supported on Docker running the following platforms:

Platform	Supported Versions
RedHat Linux	7 (32/64-bit)
CentOS	7 (32/64-bit)
SUSE	Intel 12 (64-bit)

Credential Provider on Windows (v9.9.5)

The Credential Provider for Windows is supported on the following platforms:

- Windows Server 2016
- Windows Server 2012 and Windows Server 2012 R2
- Windows Server 2008R2 (32/64 bit)

For developer endpoints:

- Windows 8.x
- Windows 7
- Windows XP (64-bit)

Note:
From the next version (v9.8), Windows 2003 and Windows XP will no longer be supported. Customers using these OS may continue using Credential Provider v9.7.1.

Credential Provider on zLinux (v6.0)

The Credential Provider for zLinux is supported on the following platforms:

Platform	Supported Versions
SUSE zLinux	10 and 11 (64-bit)

Credential Provider on HP-UX (Application Password Provider v4.5)

The Application Password Provider for HP-UX is currently supported on the following platforms:

Platform	Supported Versions
HP-UX	11.23 PA-Risc
HP-UX on Itanium	11i v3 (11.31)

Credential Provider compatibility

Credential Provider Version	Compatible Products
v.9.9.5	Works with the Digital Vault v7.x, v8.x ,v9.x, and v.10.x Supports Application Password SDK v5.5, v6.0, v7.0, v7.1, v7.2 , v9.5, and v9.9.5
v9.7	Works with the Digital Vault v7.x, v8.x ,v9.x, and v.10.x Supports Application Password SDK v5.5, v6.0, v7.0, v7.1, v7.2 and v9.5.
v7.2	Works with the Digital Vault, v7.x, v8.x ,v9.x, and v.10.x Supports GA versions for Application Password SDK v4.5, v5.0, v5.5, v6.0, v7.0, v7.1 and v7.2.
v7.1	Works with the Digital Vault, v7.x, v8.x ,v9.x, and v.10.x Supports GA versions for Application Password SDK v4.5, v5.0, v5.5, v6.0, v7.0, and v7.1.
v7.0	Works with the Digital Vault, v7.x, v8.x ,v9.x, and v.10.x Supports GA versions for Application Password SDK v4.5, v5.0, v5.5, v6.0, and v7.0.
v6.0	Works with the Digital Vault v7.x and v8.x. Supports GA versions for Application Password SDK v4.5, v5.0, v5.5, and v6.0.

Application Password SDKs

The Application Password SDK is supported on a machine where the Credential Provider is installed.

Application environments

The Application Password SDK is supported in the following application environments:

SDK	Platform	Latest Version	Notes
C/C++	AIX	V9.9.5	32-bit and 64-bit modules
	Solaris	V9.9.5	32-bit and 64-bit modules
	Linux	V9.9.5	32-bit and 64-bit modules
	Windows	V9.9.5	32-bit and 64-bit modules
	zLinux	V6.0	64-bit module
	HP-UX (Risc)	V4.5	32-bit module
	HP-UX (Itanium)	V4.5	32/64-bit modules
Java (v1.5.x and higher)	AIX	V9.9.5	
	Solaris	V9.9.5	
	Linux	V9.9.5	
	Windows	V9.9.5	
	zLinux	V6.0	
	HP-UX (Risc/Itanium)	V4.5	

SDK	Platform	Latest Version	Notes
CLI (Command Line Interface)	AIX	V9.9.5	
	Solaris	V9.9.5	
	Linux	V9.9.5	
	Windows	V9.9.5	
	zLinux	V6.0	
	HP-UX (Risc/Itanium)	V4.5	
.Net Framework (v2.0/3.5/4.0)	Windows	V9.9.5	
COM	Windows	V9.9.5	32-bit and 64-bit modules

For information about upgrading from an existing PVToolkit implementation to the Credential Provider, contact your CyberArk support representative.

Application Password SDK compatibility

Application Password SDK Version	Compatible Credential Provider Versions
v9.9.5	v9.9.5 and above
v9.7	v9.7 and above
v9.6	v9.6 and above
v9.5	v9.5 and above
v7.2	v7.2 and above
v7.1	v7.1 and above
v7.0	v7.0 and above
v6.0	v6.0, and above

Application Server Credential Provider

The Application Server Credential Provider (ASCP) is an additional component that securely and automatically manages application server credentials that are stored inside data source XML files. Using this component, you do not need to perform any code changes to applications in order to store your passwords securely in the Enterprise Password Vault, and you can perform automatic password replacement with no need to restart the Application Server, thus eliminating downtime.

Application Server Credential Provider

This version of the Credential Provider includes the following versions of the Application Server Credential Provider:

Platform	Latest ASCP JDBC Driver Proxy Version	Latest ASCP Credential Mapper Version
WebSphere	-	V7.1
WebLogic	V10.1	V5.5 p1
JBoss	V10.1	V7.2
Tomcat	V5.5	-
WebSphere Liberty	-	V9.8

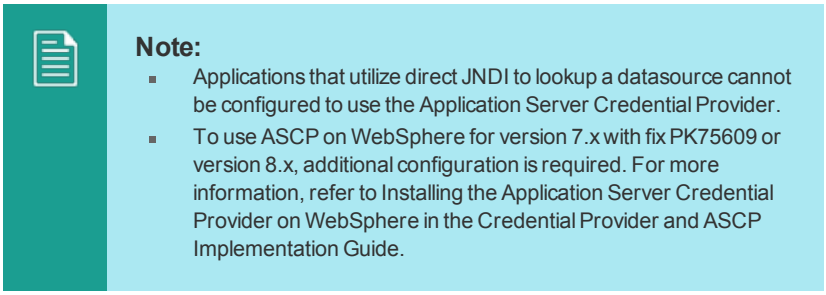
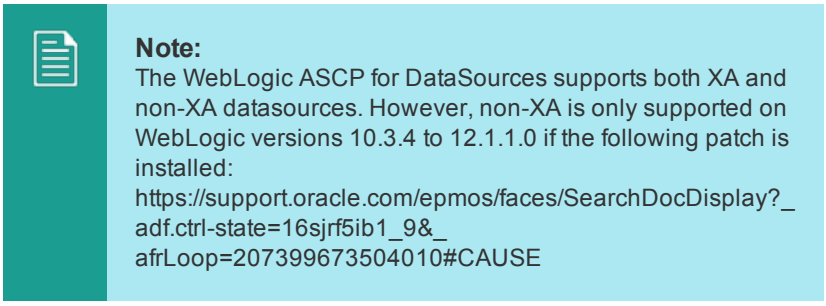
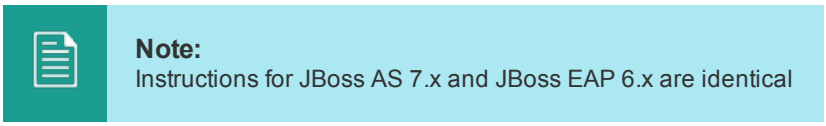
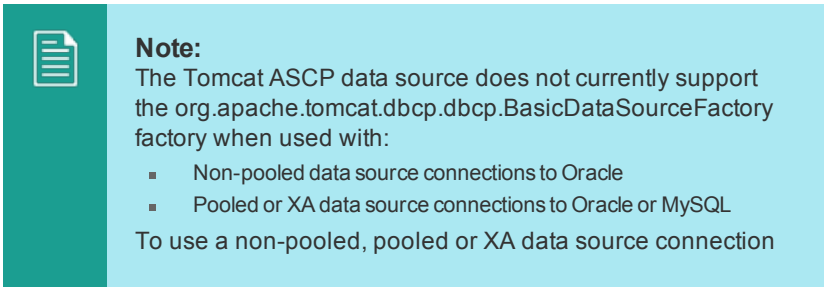
Certified Platforms

The ASCP JDBC Driver Proxy is certified on the following platforms:

Application Server	JBoss	WebLogic
AS Version	EAP 4.3 (with Java version 1.6 or above), AS 5	11g, 12c
Data Sources	local-tx-datasource, xa datasource	Generic
Databases	Oracle, msSQL, DB2	Driver & XA
Connection types	Oracle, msSQL, DB2	Driver & XA

Supported Platforms

The Application Server Credential Provider is supported on the following platforms for the above environments:

Platform	Supported Versions
IBM WebSphere	7.x, 8.0 and 8.5  **Note:** ▪ Applications that utilize direct JNDI to lookup a datasource cannot be configured to use the Application Server Credential Provider. ▪ To use ASCP on WebSphere for version 7.x with fix PK75609 or version 8.x, additional configuration is required. For more information, refer to Installing the Application Server Credential Provider on WebSphere in the Credential Provider and ASCP Implementation Guide.
Oracle WebLogic:	▪ The Application Server Credential Provider for DataSources is supported on WebLogic 9.x, 10.x, 11g (10.3.x) and 12c (12.x)  **Note:** The WebLogic ASCP for DataSources supports both XA and non-XA datasources. However, non-XA is only supported on WebLogic versions 10.3.4 to 12.1.1.0 if the following patch is installed: https://support.oracle.com/epmos/faces/SearchDocDisplay?_adf.ctrl-state=16sjrf5ib1_9&_afrLoop=207399673504010#CAUSE ▪ The Application Server Credential Provider for LDAP Authenticator is supported on WebLogic 9.x, 11g (10.3.x) and 12c (12.x)
JBoss	▪ AS 4.x, 5.x, 6.x and 7.x, EAP 6.x and WildFly 8 and 9  **Note:** Instructions for JBoss AS 7.x and JBoss EAP 6.x are identical
Tomcat	6.0, 7.0 and 8.0  **Note:** The Tomcat ASCP data source does not currently support the org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory factory when used with: ▪ Non-pooled data source connections to Oracle ▪ Pooled or XA data source connections to Oracle or MySQL To use a non-pooled, pooled or XA data source connection

Platform	Supported Versions
	to Oracle, we recommend using either the OracleFactory or the “Tomcat JDBC” data source. To use a Pooled or XA data source connection to MySQL, we recommend using either the MySQLFactory or the “Tomcat JDBC” data source.

Required Java Versions

- All ASCPs require JRE 1.5.x or higher

Supported environments

The Application Server Credential Provider is currently supported in the following environments:

- Solaris
- Linux
- Windows
- AIX

For more details about platforms that support the Provider, see Credential Provider, page 57.

Application Server Credential Provider compatibility

The CyberArk Application Server Credential Provider requires the following component to be installed on the same machine:

- Credential Provider, version 6.0 or higher

Central Credential Provider

Supported platforms

The Central Credential Provider is supported on the following platforms:

- Windows 2012 and Windows 2012 R2
- Windows 2008R2 (32/64 bit)
- Windows 2003 (32-bit)

Note:
From the next version (v9.8), Windows 2003 will no longer be supported. Customers using this OS may continue using Credential Provider v9.7.1

CyberArk compatibility

The Central Credential Provider works with the Digital Vault, v7.x, v8.x , v9.x, and v10.x.

Prerequisites

- To authenticate applications using Windows domain users, the Central Credential Provider must be in the same domain as the requesting application machines. Alternatively, the requesting application domain must be trusted by the Central Credential Provider domain. For more information about authenticating applications with the Windows domain users, refer to *Authenticating Applications* in the *Credential Provider and ASCP Implementation Guide*.
- Make sure Windows IIS 7.5 supports IIS 6.0 compatibility mode.

Client requirements

The Central Credential Provider works with application on any operating system, platform or framework that can invoke SOAP web service requests.

.NET Framework

Support for v4.5.2

On-Demand Privileges Manager

The On-Demand Privileges Manager (OPM) enables you to run privileged UNIX commands in an audited and controlled way. The On-Demand Privileges Manager must be installed on each managed UNIX system.

Note:
CyberArk may choose not to provide maintenance and support services for CyberArk's On-Demand Privileges Manager with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Supported platforms

The OPM is currently supported on the following platforms:

Platform	Latest Version
AIX	V10.4
Solaris	V10.4
Linux	V10.4
HPUX	V9.9
Windows	V10.4

OPM Supported Platforms	Supported Platforms
OPM on AIX (v10.4)	. AIX 6.1 and 7.1 TL1, TL2, and TL3 (64-bit)  **Note:** The AIX version must include the Linux Toolbox for AIX. This is built-in for AIX.
OPM on Solaris (v10.4)	. Solaris Intel 10 and 11 (SunOS 5.10 and 5.11 64-bit) . Solaris SPARC 10 and 11 64-bit (SunOS versions 5.10 and 5.11 64-bit)
OPM on Linux (v10.4)	▪ RedHat 5, 6 and 7 (32/64-bit) ▪ SUSE-Intel/ppc64le 11, 12 (ppc = powerpc) ▪ SUSE 12 on IBM Power8 (Little Endian) 64-bit

OPM Supported Platforms	Supported Platforms
	▪ Fedora 24, 25 and 26 (32-bit) ▪ CentOS 6 and 7 (32/64-bit) ▪ Oracle 5, 6 and 7
OPM on HPUX (v9.9)	Itanium/RISC v11.23 and higher
Windows	Windows platforms are supported through CyberArk Endpoint Privilege Manager. For details, see the *Endpoint Privilege Manager Implementation Guide*

OPM Compatibility

OPM Version	Compatible Digital Vault Versions
v10.x	v7.x, v8.x, v9.x and v10.x
v9.x	v7.x, v8.x, v9.x and v10.x
v7.2	v7.x, v8.x and v9.x
v7.1	v7.x, v8.x and v9.x
v7.0	v7.x, v8.x and v9.x
v6.0	v7.x, v8.x and v9.x

AD Bridge capabilities

AD Bridge connections are supported on the following platforms:

- RedHat Linux
- CentOS
- AIX
- Solaris

The following CyberArk component versions are required:

- Digital Vault Server, version 9.8 or higher
- Password Vault Web Access, version 9.8 or higher
- OPM, version 9.8 or higher

CyberArk Pluggable Authentication Module

The OPM Pluggable Authentication Module (OPM-PAM) is supported on the following platforms:

- RedHat Linux
- CentOS
- AIX
- Solaris

PAM Supported Platforms	Supported Platforms
PAM on AIX (v10.4)	. AIX 6.1 and 7.1 TL1, TL2, and TL3 (64-bit)  **Note:** The AIX version must include the Linux Toolbox for AIX. This is built-in for AIX.
PAM on Solaris (v10.4)	. Solaris Intel 10 and 11 (SunOS 5.10 and 5.11 64-bit)

PAM Supported Platforms	Supported Platforms
	▪ Solaris SPARC 10 and 11 64-bit (SunOS versions 5.10 and 5.11 64-bit)
PAM on Linux (v10.4)	▪ RedHat 5, 6 and 7 (32/64-bit) ▪ SUSE-Intel/ppc64le 11, 12 (ppc = powerpc) ▪ SUSE 12 on IBM Power8 (Little Endian) 64-bit ▪ Fedora 24, 25 and 26 (32-bit) ▪ CentOS 6 and 7 (32/64-bit) ▪ Oracle 5, 6 and 7

The OPM-PAM has the following dependencies:

- The On-Demand Privileges Manager (OPM) must be installed on the machine.

The OPM-PAM works with the following CyberArk components:

- CyberArk Digital Vault version 9.8 and higher
- OPM version 9.8 and higher

Password Upload Utility

The Password Upload utility uploads multiple password objects to the Digital Vault, making the Privileged Access Security implementation process quicker and more automatic.

Note:
CyberArk may choose not to provide maintenance and support services for CyberArk's Password Upload Utility with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Supported platforms

The Password Upload utility can be run on the following platforms:

- Windows 2008 R2 (64-bit)
- Windows 7 (64-bit)
- Windows 2003 (32-bit)
- Windows XP (32-bit)

CyberArk components

The Password Upload utility requires the following CyberArk components:

- PrivateArk Command Line Interface (PACLI), version 4.1 or higher – PACLI must be installed in the same folder as the Password Upload utility or in a folder specified in the Path.

CyberArk component compatibility

The Password Upload utility runs with the following CyberArk components:

- Digital Vault server, version 4.1 or higher

CyberArk SDKs

The CyberArk SDKs enable Privileged Access Security users and applications/scripts to access the Digital Vault server from any location, in an extremely intuitive command line environment.

Note:
CyberArk may choose not to provide maintenance and support services for CyberArk's SDKs with relation to any of the platforms and systems listed below which have reached their formal End-of-Life date, as published by their respective vendors from time to time. For more details, contact your CyberArk support representative.

Minimum requirements

The minimum requirements for all the SDK interfaces are as follows:

Disk space:	10MB free disk space
Minimum memory:	32MB
Communication:	TCP/IP connection to the Digital Vault Server

CyberArk Component compatibility

The CyberArk SDKs work with the Digital Vault server, version 4.5 and above.

Digital Vault server SDK

The Digital Vault Server SDK (PACLI) can be used on any Privileged Access Security implementation.

CyberArk Command Line Interface (PACLI)

PACLI v7.2 is currently supported on the following platforms:

- Windows 2012 R2
- Windows 2008 R2 (64-bit)
- Windows 7 (64-bit)
- Windows 2003 (32-bit)

Authentication

The Privileged Access Security solution supports a variety of authentication methods on its different interfaces:

This list may be updated frequently as additional authentication methods are supported. Please contact CyberArk Customer Support for updated information.

For more details about any of these authentication methods, see the Privileged Access Security Installation Guide .

Password Vault Web Access

Authentication methods

- Password
- Windows
- Radius
- PKI
- RSA SecurID
- LDAP
- Oracle SSO
- SAML
- Additional third party authentication servers can be easily customized.

Authentication methods with additional password authentication

- Windows with additional password authentication
- PKI with additional password authentication
- RSA SecurID with additional password authentication
- Oracle SSO with additional password authentication

Mobile PVWA authentication methods

- Password
- Radius
- RSA SecurID
- LDAP

PrivateArk Client

Authentication methods

- Password
- Windows
- Radius
- PKI
- LDAP

Central Policy Manager

Authentication methods

- Password
- Password with a certificate on a hardware token
- Radius
- PKI on Windows

Password Upload Utility

Authentication methods

- Password
- Password with a certificate on a hardware token
- Radius
- PKI on Windows

Digital Vault Server SDK (PACLI)

Authentication methods

- Password
- Password with a certificate on a hardware token
- Radius
- PKI on Windows
- RSA SecurID (only PACLI, as secondary authentication)

Privileged Access Security SDK

Authentication methods

- Password
- Radius
- SAML
- PSMP with SSH keys

Network Ports Overview

The Privileged Access Security components communicate through a variety of ports which ensure that all their communication is secure and according to the patented CyberArk protocol.

Network Port Definitions for CyberArk Components

The following tables list the network port definitions for each component in relation to the other Privileged Access Security components and managed devices.

Part 1:

	Target			
Source	**Vault**	**DR**	**CPM**	**PVWA**
Vault	×	TCP/1858 [1]	×	×
Disaster Recovery Vault (DR)	TCP/1858 [1]	×	×	×
Central Policy Manager (CPM)	TCP/1858 [1]	TCP/1858 [1]	×	×
Password Vault Web Access (PVWA)	TCP/1858 [1]	TCP/1858 [1]	×	×
Privileged Session Manager (PSM)	TCP/1858 [1]	TCP/1858 [1]	×	×
Credential Provider	TCP/1858 [1]	TCP/1858 [1]	×	×
On-Demand Privileges Manager (OPM)	TCP/1858 [1]	TCP/1858 [1]	×	×
User (Administrator)	TCP/1858 [1]; opt. Remote Administration [2]	TCP/1858 [1]; opt. Remote Administration [2]	TCP/3389	TCP/80 TCP/443 TCP/3389

× – Not relevant

[1] Default port. This can be changed, e.g. to TCP/443.

[2] Remote Administration Boards, e.g. like HP iLO, IBM RSA, Dell DRAC, etc., for virtualized environments allow access to VM Server.

[3] Refer to Standard Ports and Protocols, page 81.

[4] Depending on devices managed through direct access (Administrators' Workstations to target devices).

Part 2:

	Target				
Source	**PSM**	**Credential Provider**	**OPM**	**SMTP Server (for Event Notification)**	**Manage Target Devices, e.g. Server, Router, …**
Vault	×	×	×	TCP/25	×
Disaster Recovery Vault (DR)	×	×	×	TCP/25	×
Central Policy Manager (CPM)	×	×	×	×	See footnotes below [3]
Password Vault Web Access (PVWA)	×	×	×	×	×
Privileged Session Manager (PSM)	×	×	×	×	TCP/3389 or TCP/22
Credential Provider	×	×	×	×	×
On-Demand Privileges Manager (OPM)	×	×	×	×	×
User (Administrator)	TCP/443 TCP/3389	×	×	×	TCP/22, TCP/3389, etc. [4]

× – Not relevant

[1] Default port. This can be changed, e.g. to TCP/443.

[2] Remote Administration Boards, e.g. like HP iLO, IBM RSA, Dell DRAC, etc., for virtualized environments allow access to VM Server.

[3] Refer to Standard Ports and Protocols, page 81.

[4] Depending on devices managed through direct access (Administrators' Workstations to target devices).

Network Port Definitions for Third Party Components

The following tables list the network port definitions for various third party components that communicate with the Privileged Access Security components.

Part 1:

	Optional Target		
Source	**LDAP/S**	**RADIUS**	**RSA SecurID**
Vault	TCP/389 or TCP/636	UDP/1812 UDP/1813	UDP/5500 UDP/5560 TCP/5500 TCP/5560
Disaster Recovery Vault (DR)	TCP/389 or TCP/636	UDP/1812 UDP/1813	UDP/5500 UDP/5560 TCP/5500 TCP/5560
Central Policy Manager (CPM)	×	×	×
Password Vault Web Access (PVWA)	×	×	×
Privileged Session Manager (PSM)	×	×	×
Credential Provider	×	×	×
On-Demand Privileges Manager (OPM)	×	×	×
User (Administrator)	×	×	×

Part 2:

	Optional Target			
Source	**Backup**	**Syslog**	**NTP**	**SNMP**
Vault	Depending on backup software used	TLS/514 TCP/514 UDP/514	UDP/123	UDP/161 UDP/162
Disaster Recovery Vault (DR) or Satellite Vault	Depending on backup software used	TLS/514 TCP/514 UDP/514	UDP/123	UDP/161 UDP/162
Central Policy Manager (CPM)	×	×	UDP/123	×
Password Vault Web Access (PVWA)	×	×	UDP/123	×
Privileged Session Manager (PSM)	×	×	UDP/123	×
Credential Provider	×	×	×	×
On-Demand Privileges Manager (OPM)	×	×	×	×
User (Administrator)	×	×	×	×

Standard Ports and Protocols

The Privileged Access Security solution uses standard ports and protocols to communicate with different devices.

In this section:

Standard CPM Ports and Protocols

The following table lists the standard ports used by the CPM to communicate with the different devices whose passwords it manages automatically.

Operating Systems

Device	Protocol	Port
Windows Domain Accounts	Windows	139
	Windows	445
Windows Desktop Accounts	Windows	135
	Windows	445
	Windows	If the 'VerifyMachine NameBeforeAction' parameter is set to 'Yes': 135 High ports
Windows Local Accounts	Windows	139
	Windows	445
	Windows	If the 'VerifyMachine NameBeforeAction' parameter is set to 'Yes': 135 High ports
Windows Local Accounts over WMI	Windows	135
	Windows	445
	Windows	High ports
Windows Services	Windows	135
	Windows	445
	Windows	High ports
Windows Scheduled Tasks	Windows 2003	445
Windows IIS Application Pools	Windows	135
	Windows	445
	Windows	49154
COM+ Applications	Windows	135
	Windows	445
	Windows	High ports

Device	Protocol	Port
Windows IIS Directory Security (Anonymous Access)	Windows	135
	Windows	445
	Windows	High ports
UNIX	SSH	22
	Telnet	23
AS400	iSeries Access for Windows	449 and 8476
OS/390	FTP	21
	SSH	22
	Telnet	23
ESXi	HTTP	80
	HTTPS	443

Databases

Device	Protocol	Port
ODBC	Can be changed, depending on the database	Can be changed, depending on the database
Oracle	Proprietary protocol	1521
MSSql	Proprietary protocol	1433
MySql	Proprietary protocol	3306
Sybase	Proprietary protocol	5000
DB2	Windows 2003	445
	Unix SSH	22
	Unix Telnet	23
Informix	Windows 2003	445
	Unix SSH	22
	Unix Telnet	23
Windows Registry	Windows	135
	Windows	445
	Windows	High ports

Remote Access

Device	Protocol	Port
HP iLO	SSH	22
	Telnet	23
Dell DRAC	SSH	22

Security Appliances

Device	Protocol	Port
CheckPoint Firewall-1 NG	OPSEC	18190
RSA Authentication Manager Accounts	SSH	22
	HTTPS	443

Netscreen

Device	Protocol	Port
Netscreen	SSH	22
	Telnet	23

Network Devices

Device	Protocol	Port
CISCO	SSH	22
	Telnet	23

Directories

Device	Protocol	Port
Novell eDirectory	LDAP plain protocol	389
	LDAP secured protocol	636
SunOne Directory	LDAP plain protocol	389
	LDAP secured protocol	636

Applications

Device	Protocol	Port
CyberArk	CyberArk	1858 (can be changed)
SAP		3342

LDAP (for auto-detection processes)

Device	Protocol	Port
LDAP	Plain	389
	SSL	636

Standard Ports used for Accounts Discovery

The CyberArk CPM Scanner uses the following ports to discover accounts and SSH keys on remote machines:

Port	Use case
22	To connect to target machines using SSH. This port can be configured by the SSHPort parameter in the CACPMScanner.exe.config file.
88	Used for KDC services (only relevant to domain controllers). This port must be accessible both through network-based and host-based firewalls.
135, 137, 138, 139	To connect to target machines using NetBIOS ports. These ports must be accessible on host-based firewalls.
389	To connect to target machines using the LDAP service (only relevant to domain controllers). This port must be accessible both through network-based and host-based firewalls.
636	To connect to target machines using the LDAPS service (only relevant to domain controllers). This port must be accessible both through network-based and host-based firewalls.
445	To connect to target machines using SMB/TCP. This port must be accessible on host-based firewalls.
4431	To discover SSH keys on Windows machines without Cygwin. This port is not configurable.
49154	This port is used to view and administrate Scheduled Tasks on the remote machine.
49155, 49156	This port is used to get the list of services from the remote machine.

Standard Vault Ports and Protocols

The following table lists the standard ports and protocols used by the Vault to communicate with different devices.

Device	Protocol	Port
Remote Control	CyberArk Protocol	9022
LDAP	Plain	389
	SSL	636