Privileged Account Security System Requirements

Version 9.8

Including:

Privileged Identity Management Suite

Privileged Session Management Suite

PASSR-009-8-0-1

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 Account Security (PAS) solution. These hardware specifications are based on the entry level industry standard for small-mid range servers. For installation on a VM based environment, the requirements can be customized based on customer needs.

- *Vault and DR Vault Servers*
- *Cluster Vault and Cluster DR Vault Servers*
- *PVWA and CPM Servers*
- *PSM Servers*
- *PSMP Servers*

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

Vault and DR Vault Servers

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

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 2008 R2 SP1 (64-bit) English/German version [2] ▪ Windows 2012 R2 English/German version [2] ▪ .NET Framework 4.5.2			

[1] For more information, refer to *Privileged Session Manager®, page 30*.

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

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] .

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 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			

[1] For more information, refer to *Privileged Session Manager®, page 30*.

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

[3] Alternate clustering solutions such as VMotion cluster can be used.

PVWA and CPM Servers

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

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 ▪ Additional storage for PSM (optional) [2]	▪ 4X Eight core processors (Intel compatible) ▪ 64GB RAM ▪ 2X 80GB SAS hot-swappable drives ▪ RAID Controller ▪ Network adapter (1Gb) ▪ DVD ROM ▪ Additional storage for PSM (optional) [2]
Software prerequisites [3]			
▪ Windows 2008 R2 SP1 or Windows 2012 R2 ▪ IIS 7.5 or 8.5 ▪ .NET Framework 4.5.2 ▪ Internet Explorer 8.0, 9.0, 10.0, 11.0 ▪ PVWA and CPM can be installed on Amazon Web Services (AWS) and Microsoft Azure cloud platforms			

[1] On large scale implementations it is recommended to install the CPM and PVWA on two different machines.

[2] For more information, refer to *Privileged Session Manager®, page 30*.

[3] For specific system requirements of the different plug-ins of the Central Policy Manager, refer to the Privileged Account Security Implementation Guide.

PSM Servers

The following table lists the recommended specifications for PSM servers.

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. Refer to the Recommended Settings For Installing PSM On a Virtual Machine chapter for further instructions. ■ The maximum concurrency is lower (up to 40%) when installing the PSM server on a virtual machine.		
Software Prerequisites		

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)
■ Windows 2008 R2 SP1 or Windows 2012 R2 ■ Windows update KB2999226 ■ .NET Framework 4.5.2 ■ Microsoft Remote Desktop Services (RDS) Session Host ■ Microsoft Remote Desktop Services Gateway (optional) ■ PSM can be installed on Amazon Web Services (AWS) and Microsoft Azure cloud platforms		

PSMP Servers

The following table lists the recommended specifications for PSMP servers.

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. ■ SUSE Linux Enterprise Server 11 SP4 or 12 ■ PSM SSH Proxy can be installed on Amazon Web Services (AWS) and Microsoft Azure cloud platforms		

Privileged Account Security Solution System Requirements

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 Account 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.

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.

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.

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

- 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 Account Security solution provides standard LDAP v3 support and has been tested and certified with the following directories:

- MS Active-Directory – Each of the following platforms is supported with its correlating functional level.
  - Windows 2003 with Service Pack 2
  - Windows 2008
  - Windows 2012
  - Windows 2012 R2
- Sun One v5.2
- IBM Tivoli Directory Server v6.0
- 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.

CyberArk Component Compatibility

The Digital Vault server works with the following CyberArk components:

- PrivateArk Client/WebClient, version 8.0.
- Central Policy Manager, version 9.8
- Password Vault Web Access, version 9.8
- Privileged Session Manager, version 9.0.1 or higher

- Privileged Session Manager SSH Proxy, versions 7.2.9 or higher
- On-Demand Privileges Manager, versions 6.0 or higher
- Credential Provider, version 4.5 or higher

Distributed Vaults Compatibility

The following CyberArk clients can run on a Satellite Vault:

- Credential Provider, version 9.7
- ExportVaultData utility, version 9.8
- PAReplicate utility, version 9.8

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

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

- Windows 2012 R2

  Note: 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.
- 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.
- 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/Web Client

Note: CyberArk may choose not to provide maintenance and support services for the PrivateArk Client/Web 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.

The PrivateArk Client/Web Client is the Windows interface for performing administrative operations in the Privileged Account Security solution, such as user management. The minimum requirements for the PrivateArk Client/Web Client are as follows:

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 Browsers

The PrivateArk Client/Web Client is currently supported on the following browsers:

- Microsoft Internet Explorer Version 8.0

Supported Platforms

The PrivateArk Client/Web Client is currently supported on the following platforms:

- 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)
- Windows Vista (32-bit)
- Windows 2003 with Service Pack 2 (32-bit)
- Windows XP with Service Pack 3 (32-bit)

Reports that are generated in the PrivateArk Client/Web 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.

The minimum requirements for the NT Authentication Agent are as follows:

- 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.

The minimum requirements for the CyberArk Vault Backup utility are as follows:

- 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.

The minimum requirements for the CyberArk Remote Control Client are as follows:

- 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)

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 Account 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.

The minimum requirements for the PVWA are as follows:

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 2012R2 Windows 2008R2 with Service Pack 1 Windows 2008R2 ■ IIS 8.5 (Windows 2012 R2) IIS 7.5 (Windows 2008 R2/Windows 2008 R2 SP1) ■ Internet Explorer 8.0, 9.0, 10.0 and 11.0 ■ .NET Framework 4.5.2

Supported Browsers

The following browsers support the PVWA application:

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

Notes:

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

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

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

- Chrome: Any version released in the last six months

Supported Connections

- PSM and EPV transparent 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 and Helsinki
- BMC Remedy v9.1

For information about configuring other ticketing systems, refer to the Privileged Account Security Implementation Guide.

Requirements on End-user Machines

- RDP ActiveX Client 5.2 or higher (for PSM connections and for EPV RDP transparent connections for users working from IE)
- 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) 1.4 or higher (for SSH transparent connections)
- Adobe Flash player 10.0 browser add-on or higher (for PSM Direct Playback)

Notes:

- For PSM Connections from Unix desktops or connections that need NLA authentication and for EPV RDP transparent connections for users working from a non-Windows environment, 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 and EPV RDP Connections that Require an External Tool in the Privileged Account Security Implementation Guide.

Supported Mobile Devices

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

- iPhone Smartphones
- Blackberry Smartphones
- Android-powered Smartphones

Supported Languages

The PVWA supports the following languages:

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

CyberArk Component Compatibility

The PVWA works with the following CyberArk components:

- Digital Vault Server, version 9.8
- Central Policy Manager, version 9.8
- Privileged Session Manager, version 9.0.1 or higher
- Privileged Session Manager SSH Proxy, versions 7.2.9 or higher
- On-Demand Privileges Manager, versions 6.0 or higher
- Credential Provider, version 4.5 or higher

Requirements for Accounts Feed

Scanning 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 2003, 2008, 2012

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

Credentials for Scanning

- In the Active Directory:
  - Read permissions in the OU to scan and all sub-OUs
- On target machines:
  - Domain Administrator

  or,
  - 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

- Workstations:
  - Windows 2000
  - Windows XP
  - Windows Vista
  - Windows 7
  - Windows 8
  - Windows 10
- Servers:
  - Windows 2000
  - Windows 2003
  - Windows 2008
  - Windows 2012
  - Windows 2016

Supported Target Computers for Discovering Dependencies

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

Notes:

- 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

The following protocols 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 information about how to enable the Windows (WMI) Protocol in your environment, see *Appendix G: Enabling WMI Ports on Windows Client Machines* in the *Privileged Account 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 60*.

Scanning for Unix Accounts

Discovery processes detect the following Unix accounts:

- Local accounts

  Note: Domain users that are used to authenticate 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, psrinfo, wc, find, xargs, ssh-keygen, ls, rm, truss, hostname, ifconfig All account details	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.

To Enable the Windows (WMI) Protocol in your Environment

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.
   - **Windows XP** - Run the following commands from the commands prompt:
     - netsh firewall set service RemoteAdmin enable.
     - netsh firewall add portopening protocol=tcp port=135 name=DCOM_ TCP135.
     - netsh firewall set portopening tcp 445 smb enable.

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 Account Security component and does not require a dedicated machine. However, it must be installed on a machine that is accessible to the network.

The minimum requirements for the Central Policy Manager are as follows:

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 2012R2 Windows 2008 R2 with Service Pack 1 ■ Internet Explorer 8.0, 9.0, 10.0 and 11.0

For specific system requirements of the different plug-ins of the Central Policy Manager, refer to the Privileged Account Security Implementation Guide.

CyberArk Component Compatibility

The Central Policy Manager works with the following CyberArk components:

- Digital Vault server, version 9.8
- Password Vault Web Access, version 9.8
- 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 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:

- Windows Domain users:
  - Windows 2012/2012R2 Active Directory server
  - Windows 2008/2008R2 with Service Pack 1 Active Directory server
  - Windows 2000/2003 server
- Windows Local users:
  - Windows 2016 server - only local administrators
  - Windows 2012/2012R2 server
  - Windows 2008/2008R2 server with Service Pack 1
  - Windows 2000/2003 server
  - Windows 10
  - Windows 8
  - Windows 7 with Service Pack 1
  - Windows XP/Vista
- Windows Local users with WMI:
  - Windows 2016 server
  - Windows 2012/2012R2 server
  - Windows 2008 server
  - Windows 2000/2003 server
  - Windows 10
  - Windows 8
  - Windows 7
  - Windows XP/Vista
- Windows Applications:
  - Services:
    - Windows:
      - Windows 2016 server
      - Windows 2012/2012R2
      - Windows 2008/2008R2 with Service Pack 1
      - Windows 2000/2003
      - Windows 10
      - Windows 8
      - Windows 7 with Service Pack 1
      - Windows XP/Vista
    - Microsoft SQL Server:
      - Microsoft SQL Server 2005/2008
    - Microsoft SQL Cluster Service:
      - Microsoft SQL Cluster Service 2005/2008
  - Windows Scheduled Tasks
    - Windows 2016 server

- Windows 2012/2012R2
- Windows 2008/2008R2 with Service Pack 1
- Windows 2000/2003
- Windows 10
- Windows 8
- Windows 7 with Service Pack 1
- Windows XP/Vista

Notes:

- 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 2012/2012R2
  - Windows 2008/2008R2 with Service Pack 1 (with "IIS 6 management compatibility" role service)
  - Windows 2003
- Windows IIS Directory Security (Anonymous Access)
  - Windows 2016 server
  - Windows 2012/2012R2
  - Windows 2008/2008R2 with Service Pack 1
  - Windows 2003
- COM+ Applications
  - Windows 2016 server
  - Windows 2012/2012R2
  - Windows 2008/2008R2 with Service Pack 1
  - Windows 2003

- Unix passwords:
  - Solaris Intel 9, 10, 11
  - Solaris Sparc 9
  - 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

    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:

- 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.
- Microsoft SQL Server passwords:
    - Microsoft SQL Server 7, 2010, 2012, 2014 or higher
      Note: For higher versions, additional customizations may be required.
- Sybase database passwords:
    - Sybase Adaptive Server Enterprise 12.5.2
      Note: For higher versions, additional customizations may be required.
- MySQL Server passwords:
    - MySQL version 5 and above
    - Connector/ODBC v3.51.28 (32-bit) driver
- DB2 passwords:
    - Windows platforms:
        - IBM DB2 on Windows XP, Windows 2000, 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 XP, Windows 2000, 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.

Security Appliances

- CheckPoint Firewall-1 NG passwords:
  - CheckPoint Firewall-1
- NetScreen Firewall passwords:
  - NetScreen version 5.3.0r2.0

    Note: For higher versions, additional customizations may be required.
- RSA Authentication Manager Accounts
  - RSA Authentication Manager 8.1

Network Devices

- 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

- Novell eDirectory Passwords:
  - Novell eDirectory version 8.7.1 SMP or higher
- SunOne Directory Passwords:
  - SunOne Directory Server version 5.2

Applications

- 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

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:

- Digital Vault server, version 9.8
- Password Vault Web Access, version 9.8
- Central Policy Manager, version 9.8
- 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

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

Credentials for Scanning SSH Keys

In order 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 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 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 2012R2 Windows 2008R2 with Service Pack 1 ■ .NET Framework 4.5.2 ■ 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 Account 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 Account Security Implementation Guide.

- Unix, Linux and Network devices using the following protocols:
  - SSH (including file-transfer capabilities)
  - Telnet
- Windows RDP (including file-transfer capabilities)
- 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 and 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 and v10.6.1.3
  - 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:
  - SQL Server Management Studio 2008 and 2012
- 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, and v5.0

Storage Requirement on the Digital Vault Server

The Privileged Session Manager stores the session recordings on the Digital Vault server. 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:

- 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
- 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.

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 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 Privileged Session Manager SSH Proxy (PSMP) is a CyberArk component that enables you to secure, control and monitor privileged access to network 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 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. ■ 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 7.3 server.

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:

- 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
- 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:

- 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:

- 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

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.

The Credential Provider is currently supported on the following platforms:

Platform	Latest Version
AIX	V9.7.1
Solaris	V9.6
Linux	V7.2 V9.7.1 V9.8
Windows	V9.7.1
zLinux	V6.0
HP-UX [1]	V4.5

Credential Provider on AIX (v9.7.1)

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

- AIX 5.3 TL9, 6.0, 6.1, and 7.1 TL1, TL2, and TL3 (64-bit)

Notes:

- The AIX version must include the Linux Toolbox for AIX. This is built-in for AIX 5.3 TL9 and higher.
- From the next version, AIX 5.3 will no longer be supported as it has reached its End of Life by the vendor. Customers using this OS may continue using the Credential Provider v9.6.

[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 Solaris (v9.6)

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

- Solaris Intel 11 (SunOS 5.11)
- Solaris Intel 10 (SunOS 5.10 64-bit)
- Solaris Intel 9 (SunOS 5.9 32-bit)
- Solaris SPARC 9, 10,11 64-bit (SunOS versions 5.9, 5.10 and 5.11 64-bit)

Note: From the next version, Solaris 9 (both Intel and SPARC) will no longer be supported as it has reached its End of Life by the vendor. Customers using this OS may continue using Credential Provider v9.6.

Credential Provider on Linux (v9.8)

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

- RedHat Linux 4, 5, 6 and 7 (32/64-bit)
- SUSE-Intel 10, 11 and 12 (64-bit)
- Fedora 8 (32-bit)
- Fedora 13 and 14 (32-bit)
- CentOS 4, 5, 6 and 7 (32/64-bit)

Credential Provider on Linux (v9.7.1)

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

- SUSE-Power PC 12 (Little Endian) 64-bit
- RHEL-Power PC 7.1 (Little Endian) 64-bit

Credential Provider on Linux (v7.2)

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

- Ubuntu 12.04 LTS 64-bit

Credential Provider on Docker (1.11)

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

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

Credential Provider on Windows (v9.7.1)

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

- Windows 2012 and Windows 2012 R2
- Windows 2008R2 SP1 (32/64 bit)
- Windows 2003 SP2 (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.

For developer endpoints:

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

Note: From the next version (v9.8), Windows XP will no longer be supported. Customers using this 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:

- 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:

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

Credential Provider Compatibility

- Credential Provider v9.7
  - The Credential Provider v9.7 works with the Digital Vault v7.x, v8.x and v9.x.
  - The Credential Provider v9.7 supports Application Password SDK v5.5, v6.0, v7.0, v7.1, v7.2 and v9.5.
- Credential Provider v7.2
  - The Credential Provider v7.2 works with the Digital Vault, v7.x, v8.x and v9.x.
  - The Credential Provider v7.2 supports GA versions for Application Password SDK v4.5, v5.0, v5.5, v6.0, v7.0, v7.1 and v7.2.
- Credential Provider v7.1
  - The Credential Provider v7.1 works with the Digital Vault, v7.x, v8.x and v9.x.
  - The Credential Provider v7.1 supports GA versions for Application Password SDK v4.5, v5.0, v5.5, v6.0, v7.0, and v7.1.
- Credential Provider v7.0
  - The Credential Provider v7.0 works with the Digital Vault, v7.x, v8.x and v9.x.
  - The Credential Provider v7.0 supports GA versions for Application Password SDK v4.5, v5.0, v5.5, v6.0, and v7.0.
- Credential Provider v6.0
  - The Credential Provider v6.0 works with the Digital Vault v7.x and v8.x.
  - The Credential Provider v6.0 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.

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

SDK	Platform	Latest Version	Notes
C/C++	AIX	V9.7	32-bit and 64-bit modules
	Solaris	V9.7	32-bit and 64-bit modules
	Linux	V9.8	32-bit and 64-bit modules
	Windows	V9.7	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	V9.7	
	Solaris	V9.7	
	Linux	V9.8	
	Windows	V9.7	
	zLinux	V6.0	
	HP-UX (Risc/Itanium)	V4.5	
CLI (Command Line Interface)	AIX	V9.7	
	Solaris	V9.7	
	Linux	V9.8	
	Windows	V9.7	
	zLinux	V6.0	
	HP-UX (Risc/Itanium)	V4.5	
.Net Framework (v2.0/3.5/4.0)	Windows	V9.7	
COM	Windows	V9.7	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

- The Application Password SDK v9.7 is supported on the Credential Provider v9.7 and up.
- The Application Password SDK v9.6 is supported on the Credential Provider v9.6 and up.
- The Application Password SDK v9.5 is supported on the Credential Provider v9.5 and up.
- The Application Password SDK v7.2 is supported on the Credential Provider v7.2 and up.
- The Application Password SDK v7.1 is supported on the Credential Provider v7.1 and up.
- The Application Password SDK v7.0 is supported on the Credential Provider v7.0 and up.
- The Application Password SDK v6.0 is supported on the Credential Provider v6.0, and up.

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.

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

Platform	Latest Version
WebSphere	V9.6
WebLogic	V5.5 p1
JBoss	V7.2
Tomcat	V5.5
WebSpere Liberty	V9.8

Supported Platforms

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

- IBM WebSphere 7.x, 8.0 and 8.5

Notes:

- 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 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, refer to *Credential Provider, page 35*.

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

The Central Credential Provider is supported on the following platforms:

- Windows 2012 and Windows 2012 R2
- Windows 2008R2 SP1 (32/64 bit)
- Windows 2003 SP2 (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 and v9.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.

On-Demand Privileges Manager

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.

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.

The OPM is currently supported on the following platforms:

Platform	Latest Version
AIX	V9.6
Solaris	V9.6
Linux	V9.6
Windows	V9.6

OPM Supported Platforms	Supported Platforms
OPM on AIX (v9.6)	▪ AIX 5.3 TL9, 6.0, 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 5.3 TL9 and higher.
OPM on Solaris (v9.6)	▪ Solaris Intel 10 (SunOS 5.10 64-bit) ▪ Solaris Intel 9 (SunOS 5.9 32-bit) ▪ Solaris SPARC 8, 9, 10 64-bit (SunOS versions 5.8, 5.9, 5.10 and 5.11 64-bit) **Note:** On Solaris 8 only, install patch 112438-03 (random number generator) or higher. Reboot the Solaris machine after installing this patch.
OPM on Solaris (v9.7)	▪ Solaris Intel 10 and 11 (SunOS 5.10 and 5.11 64-bit) ▪ Solaris Intel 9 (SunOS 5.9 32-bit) ▪ Solaris SPARC 8, 9, 10 and 11 64-bit (SunOS versions 5.8, 5.9, 5.10 and 5.11 64-bit)
OPM on Linux (v9.6)	▪ RedHat Linux 4, 5, 6 and 7 (32/64-bit) ▪ SUSE-Intel 10 and 11 (64-bit) ▪ SUSE 12 on IBM Power8 ▪ Fedora 13 and 14 (32-bit) ▪ CentOS 4, 5, and 6 (32/64-bit)

OPM Supported Platforms	Supported Platforms
OPM on Windows (v5.5)	Window Server platforms: ■ Windows 2012 and Windows 2012 R2 ■ Windows 2008 (32/64-bit) ■ Windows 2008 R2 (64 bit) ■ Windows 2003 SP2 (32/64-bit)
	Window Desktop platforms: ■ Windows 10 ■ Windows 8.1 (32/64-bit) ■ Windows 8 (32/64-bit) ■ Windows 7 (32/64-bit) ■ Windows Vista SP1 ■ Windows XP SP3

OPM Compatibility

- OPM v9.6
  - OPM v9.6 works with the Digital Vault v7.x, v8.x and v9.x.
- OPM v9.5
  - OPM v9.5 works with the Digital Vault v7.x, v8.x and v9.x.
- OPM v7.2
  - OPM v7.2 works with the Digital Vault v7.x, v8.x and v9.x.
- OPM v7.1
  - OPM v7.1 works with the Digital Vault v7.x, v8.x and v9.x.
- OPM v7.0
  - OPM v7.0 works with the Digital Vault v7.x, v8.x and v9.x.
- OPM v6.0
  - OPM v6.0 works with the Digital Vault v7.x, v8.x and v9.x.

AD Bridge Capabilities

AD Bridge connections are supported on the following platforms:

- RHEL 4, 5, 6, 7

The following CyberArk component versions are required:

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

Password Upload Utility

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.

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

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

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.

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

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 Account Security implementation.

CyberArk Command Line Interface (PACLI)

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

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

Authentication

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

- *Password Vault Web Access*
- *PrivateArk Client*
- *Central Policy Manager*
- *Password Upload Utility*
- *Digital Vault Server SDK*
- *Privileged Account Security SDK*

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

For more information about any of these authentication methods, refer to the Privileged Account Security Installation Guide.

Password Vault Web Access

The PVWA supports the following authentication methods:

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

In addition, the PVWA supports the following 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

The Mobile PVWA supports the following authentication methods:

- Password
- Radius
- RSA SecurID
- LDAP

PrivateArk Client

The PrivateArk Client supports the following authentication methods:

- Password
- Windows
- Radius
- PKI
- LDAP

Central Policy Manager

The Central Policy Manager supports the following authentication methods:

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

Password Upload Utility

The Password Upload Utility supports the following authentication methods:

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

Digital Vault Server SDK

The Digital Vault Server SDK (PACLI) supports the following authentication methods:

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

Privileged Account Security SDK

The Privileged Account Security SDK supports the following authentication methods:

- Password
- Radius
- SAML

Network Ports Overview

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

This section lists the following ports:

- *Network Port Definitions for CyberArk Components*
- *Network Port Definitions for Third Party Components*

Network Port Definitions for CyberArk Components

The following tables list the network port definitions for each component in relation to the other Privileged Account 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 55*.

[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 55*.

[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 Account 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	UDP/514	UDP/123	UDP/161 UDP/162
Disaster Recovery Vault (DR)	Depending on backup software used	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 Account Security solution uses standard ports and protocols to communicate with different devices.

- *Standard CPM Ports and Protocols*
- *Standard Ports used for Accounts Discovery*
- *Standard Vault Ports and Protocols*

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 2000	139
	Windows XP and 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 2000	139
	Windows XP and 2003	445
	Unix SSH	22
	Unix Telnet	23
Informix	Windows 2000	139
	Windows XP and 2003	445
	Unix SSH	22
	Unix Telnet	23

Device	Protocol	Port
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