BeyondTrust Privileged Identity Supported Platforms and Systems

Supported Host Platforms

Management Console and Zone Processors

Supported Host Platforms
Windows Server 2019
Windows Server 2016
Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2
Windows 10
Windows 8.1

Note: *Core Editions are not supported as hosting platforms for the management console. Workstation-classified operating systems are supported for small testing environments only.*

Virtualization

Supported Host Platforms
Hyper-V
VMware ESX
VMware Workstation

Web Application and Web Service

Supported Host Platforms
IIS 10.5
IIS 10
IIS 8.5
IIS 8
IIS 7.5

Database (Program Data Store)

Supported Host Platforms
Microsoft Azure SQL Server
Microsoft SQL Server 2019
Microsoft SQL Server 2017
Microsoft SQL Server 2016
Microsoft SQL Server 2014
Microsoft SQL Server 2012
Microsoft SQL Server 2008 R2
Microsoft SQL Server 2008

Note: *Clustered databases are fully supported and recommended.*

Note: *Microsoft SQL Express editions are supported for proof of concepts and test environments. However, we do not recommend these editions for production environments.*

Application Launcher

Supported Host Platforms
Windows Server 2019
Windows Server 2016
Windows Server 2012 R2
Windows Server 2012
Windows Server 2008 R2

Note: *Core Editions are not supported as hosting platforms for the application launcher.*

Authentication Providers

Supported Providers
Active Directory
Active Directory Federated Services (ADFS) (SAML)
Facebook (OAuth)
Google (OAuth)

Supported Providers
LDAP
Microsoft Active Directory (OAuth)
Microsoft Azure Active Directory (SAML)
OKTA SAML
OneLogin (SAML)
PingOne (SAML)
SalesForce (OAuth)
SAML (any SAML compliant vendor)

Multi-Factor Providers

Supported Providers
Certificates (Smart Cards, CAC/PIV, etc.)
DUO
OATH (built-in)
OATH compliant (Yubico)
RADIUS (RSA, DUO, etc.)
RSA SecureID (v8.x and newer)
SafeNet

Supported Target Endpoints for Password Spinning and Discovery

Windows

Supported Versions	Discovery	Password Spinning
Windows Server 2019	✓	✓
Windows Server 2016	✓	✓
Windows Server 2012 R2	✓	✓
Windows Server 2012	✓	✓
Windows Server 2008 R2	✓	✓
Windows Server 2008	✓	✓
Windows Server 2003	✓	✓
Windows 10	✓	✓
Windows 8.1	✓	✓
Windows 7	✓	✓
Windows Vista	✓	✓
Windows 2000	✓	✓
Windows XP	✓	✓

Target Databases

Supported Databases	Discovery	Password Spinning
IBM DB2	✓	✗
Maria DB	✓	✓
Microsoft SQL Server 2019	✓	✓
Microsoft SQL Server 2017	✓	✓
Microsoft SQL Server 2016	✓	✓
Microsoft SQL Server 2014	✓	✓
Microsoft SQL Server 2012	✓	✓
Microsoft SQL Server 2008 R2	✓	✓
Microsoft SQL Server 2005	✓	✓

Supported Databases	Discovery	Password Spinning
Microsoft SQL Server 2000	✓	✓
MySQL 4.x+	✓	✓
Oracle 12c	✓	✓
Oracle 11g	✓	✓
Oracle 10g	✓	✓
PostgreSQL	✓	✓
Sybase ASE	✓	✓
Teradata	✓	✓

Note: *Non-Microsoft databases require provider-specific drivers supplied by the manufacturer and cannot be shipped with BeyondTrust PI. Support for Oracle database versions also depends on the Oracle OLEDB provider.*

Linux/Unix/SSH/Telnet

Supported Vendors and Versions	Discovery	Password Spinning
Berkeley Software Distribution (BSD) (free)	✓	✓
CentOS	✓	✓
HP/UX	✓	✓
Mac OSX	✓	✓
OpenBSD	✓	✓
Red Hat	✓	✓
Solaris	✓	✓
Suse	✓	✓
Ubuntu	✓	✓
Other SSH/Telnet capable systems	✓	✓

Note: *SSH version 2.0 is required to access the system. Blowfish encryption is not supported.*

Mainframes and Other Large-Scale Systems

Supported Vendors and Versions	Discovery	Password Spinning
AS/400	✗	✓
OS/390	✗	✓
z/OS	✗	✓

Hypervisors

Supported Vendors and Versions	Discovery	Password Spinning
Microsoft Hyper-V	✓	✓
VMware ESX (SSH)	✓	✓
VMware ESXi (native or SSH)	✓	✓

Routers and Switches

Supported Vendors and Versions	Discovery	Password Spinning
Checkpoint	✗	✓
Cisco	✓	✓
EMC	✗	✓
F5	✗	✓
Fortigate	✗	✓
Foundry	✗	✓
HP Procurve	✗	✓
Juniper	✗	✓
NetApp	✗	✓
Palo Alto	✗	✓
Riverbed	✗	✓
SSH-capable Printers	✗	✓
SSH-capable Network Infrastructure (Power Distribution Units)	✗	✓
Other SSH/Telnet capable systems	✗	✓

Note: *SSH version 2.0 is required to access the system. Blowfish encryption is not supported.*

LDAP Directories

Supported Vendors and Versions	Discovery	Password Spinning
Apache LDAP Directory	✓	✓
Apple Open Directory	✓	✓
IBM Tivoli Directory	✓	✓
Microsoft Active Directory	✓	✓
Novell eDirectory	✓	✓
Open LDAP	✓	✓
Oracle Internet Directory	✓	✓
Sun One Directory Server	✓	✓
ViewDS Directory	✓	✓
Any other LDAP compliant directory	✓	✓

IPMI/iLO Cards

Supported Vendors and Versions	Discovery	Password Spinning
DELL Chassis Management Controller (CMC)	✓	✓
DELL Remote Access Card (DRAC) 3-7	✓	✓
Generic Intelligent Platform Management Interface (IPMI)	✓	✓
HP Integrated Lights Out (iLO) 1-4	✓	✓
SuperMicro IPMI	✓	✓
Any IPMI 1.5 or 2.0 compliant device	✓	✓

Cloud Service Providers

Supported Vendors	Discovery	Password Spinning
Amazon Web Services	✓	✓
Microsoft Azure Active Directory	✓	✓
Rackspace Public Cloud	✓	✓

Supported Vendors	Discovery	Password Spinning
SalesForce	✓	✓
SoftLayer	✓	✗

Other Targets

Supported Targets	Discovery	Password Spinning
IBM WebSphere	✓	✓
McAfee ePolicy Orchestrator (ePO)	✓	✓
Oracle PeopleSoft	✓	✓
Oracle WebLogic	✓	✓
Xerox Phaser Printers (via SNMP)	✓	✓

Supported Subsystem Password Propagation

Supported Subsystems	Discovery	Password Spinning
.NET Config Cache	✓	✓
Arbitrary Processes	✗	✓
Auto-logon Accounts (domain and local)	✓	✓
Java Middleware	✗	✓
Logon Cache	✓	✓
Microsoft SCOM RunAs Accounts	✓	✓
Microsoft Sharepoint	✓	✓
Microsoft SQL Reporting Services	✓	✓
SDK for Programmatic Use of Stored Credentials	✗	✓
Search String Replacement in Text or Binary Files	✗	✓
Windows Automatic Login Accounts	✓	✓
Windows: COM	✓	✓
Windows: DCOM	✓	✓
Windows: IIS 6-10.5 Application Pools (confirm app status is in the same state)	✓	✓
Windows: IIS 6-10.5 Network Credentials	✓	✓
Windows: IIS 6-10.5 Website/Virtual Directories	✓	✓
Windows: Scheduled Tasks	✓	✓
Windows: Scheduling Services AT Task System	✓	✓
Windows: Service - Clustered	✓	✓
Windows: Service - Standalone	✓	✓

Supported Integrations

Syslog

Supported Integrations
AlienVault
ARCSight (CEF)
Generic Syslog
QRadar (LEEF)
RSA Envision
Splunk
Any Syslog capable target

Help Desk

Supported Integrations
BMC Remedy
CA Service Desk
HP Service Manager
JIRA
Microsoft System Center Service Manager (SCSM)
OTRS
ServiceNow

Hardware Security Modules (HSMs)

Supported Integrations
SafeNet Aladdin
Entrust nCipher
Utimaco
Any PKCS#11 compliant HSM

Third Parties

Supported Integrations
Balabit
Core Security
FireEye

Supported Integrations
FireMon
ObserveIT
Qualys
Rapid7
Raytheon
RSA Aveksa
SailPoint
Securonix
ServiceNow
Tenable

Specific Platform Considerations

In some cases, more information about certain BeyondTrust PI-supported platforms and systems is needed in order to properly discover and manage those systems. This section describes considerations for the management targets supported by Privileged Identity.

Amazon Web Services

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to Amazon uses an Amazon account configured with an API certificate for validation. The API certificate (including alternate name and password) is used for AWS management.
Password Management	✓	
Ports and Protocols	✓	All management functions occur over an HTTPS connection. If the Privileged Identity host cannot connect directly to the internet, a proxy server connection may need to be configured upon enrollment of the AWS instance.

AS400

Considerations	Supported	Details
Account Discovery	✓	Configuration of an LDAP connector is requred for Account Discovery.
Authentication	✓	When establishing an SSH session, authentication to AS400 hosts can occur using a certificate or password. Users can originate from a local directory or from a central directory. Telnet can support password authentication only. While all scenarios are supported, each requires different considerations and planning, especially when using certificates. It is important to understand your system's authentication requirements.
Password Management	✓	
Ports and Protocols	✓	If using SSH, take into consideration the requirements for the target SSH port, for encryption, and for HMAC algorithms. If SSH is not used, the 5250 terminal is used instead. 5250 terminal emulation is supported through an add-on component provided by DN-Computing, dn-computing.com. With or without SSL, 5250 terminals run over Telnet. It is important to note which port to use and if SSL is enabled.

Cisco Devices

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	When establishing an SSH session, authentication to a Cisco device can occur using a certificate or password. Users can originate from a local directory or from a central directory. While all scenarios are supported, each requires different considerations and planning, especially when using certificates. It is important to understand your system's authentication requirements.
Password Management	✓	It is important to know which account will be managed and which account will manage it. It is also important to know the process to follow to perform that management. Management of passwords is performed using answer files. An answer file identifies what input is given to the system and what output is expected from the command. Any deviation can cause the password change job to incorrectly report the final status of the operation.
Ports and Protocols	✓	By default, Cisco devices are Telnet-enabled. However, SSH must be enabled. It is highly recommended you use SSH for all password management to avoid the transmission of clear text passwords. SSH uses a single port, which defaults to TCP 22. If you use Telnet for any reason, the default port is 23, but this can be changed. Whether using SSH or Telnet, you must know the target port and if an alternate port has been configured for use. Ports are configured in the answer files used for password management. If multiple systems are on different ports, multiple answer files are required. If using Telnet, passwords cannot be programmatically passed. Answer files must include the management steps and the login process, meaning the Telnet portion of the answer file must be edited.

IBM DB2

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to a DB2 database can be performed using any non-managed account. To make the connection, you must know the default database name.
Password Management	✗	Password management for DB2 databases is not available because the accounts DB2 use comes from the local host or from a central directory.
Ports and Protocols	✓	For most DB2 database installations, including clustered resources, there are no additional steps beyond installing the proper OLE DB provider on the Privileged Identity host performing the management. By default, DB2 listens on port 50000; however, the port can be changed.

IBM WebSphere

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported for target WebSphere instances and for accounts found in the core WebSphere product.
Authentication	✓	Authentication to a WebSphere instance must use a local WebSphere account.
Password Management	✓	Passwords for target WebSphere instances can be managed.
Ports and Protocols	✓	The port requirements for WebSphere can vary based on installation and SSL use. With SSL, the default ports used are 9080 and 9443.

Note: *An EAR file must be installed as an enterprise application to start the WebSphere instance.*

IPMI (Integrated Lights Out)

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to an IPMI device can occur using local credentials. The password for the management account must be known to Privileged Identity in order to begin management.
Password Management	✓	Privileged Identity expects the login account to be defined upon enrollment of the IPMI device. This allows BeyondTrust Privileged Identity to read all IPMI properties and to change passwords.
Ports and Protocols	✓	IPMI runs over UDP port 623. IPMI over LAN must be enabled on the target device, and the target device must conform to IPMI v1.5 or 2.0 specifications. IPMI over LAN is not always automatically enabled and may require administrative configuration to be enabled. By default, UDP port 623 is not open on routed segments protected by firewalls. You must contact your firewall administrator for assistance.

Note: *HP iLO 2 devices require BIOS revision 2.05 to be compatible with IPMI specification.*

LDAP

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported by Privileged Identity for LDAP directories. To identify accounts, you must know the proper LDAP search filter and the object identifier property for your target LDAP directory. Searches start at the base LDAP path. Assuming the base LDAP path and search filter are correct, the search may still fail if the LDAP authentication record is configured to use paged queries. The directory cannot use paged queries (or vice versa).
Authentication	✓	To authenticate to an LDAP directory, you need the following information: • **Target server**: The target server to query. • **Base LDAP path**: The base LDAP path from which to begin the query. • **Authentication type/ Log In Name and Format**: Be mindful of how the login username and password must be formatted (simple vs. not simple) as well as what authentication type is required (explicit, Integrated, etc.). • **Port and Protocols**
Password Management	✓	Privileged Identity can perform password management for LDAP users, provided the login account has the ability to reset target user passwords.
Ports and Protocols	✓	All management operations are performed via LDAP. By default, LDAP listens on port 389, but directories can be configured for alternate LDAP ports or can be cofigured to use SSL. LDAP with SSL defaults to port 636. Typically, the port configuration does not change. If it does change, SSL (or TLS) may be required when it is usually not required.

> ***Note:*** *There are four LDAP directory nodes defined in Privileged Identity. All four nodes operate the same way; however, the default search and attribute parameters can vary slightly. You may use any node for any LDAP- compliant directory you intend to discover and manage.*

Linux/Unix

Considerations	Supported	Details
Account Discovery	✓	Account discovery for Linux/Unix systems requires the ability to read from **/etc/shadow** and **/etc/password**.
Authentication	✓	When establishing an SSH session, authentication to Linux/Unix hosts can occur using a certificate or password. Users can originate from a local directory or from a central directory. While all scenarios are supported, each requires different considerations and planning, especially when using certificates. It is important to understand your system's authentication requirements.

Considerations	Supported	Details
Password Management	✓	It is important to know which account will be managed and which account will manage it. It is also important to know the process to follow to perform that management. Management of passwords is performed using answer files. An answer file identifies what input is given to the system and what output is expected from the command. Any deviation can cause the password change job to incorrectly report the final status of the operation.
Ports and Protocols	✓	Modern Linux/Unix systems use SSH as the default protocol for management operations. SSH uses a single port, which defaults to TCP 22. If you use Telnet for any reason, the default port is 23, but this can be changed. Whether using SSH or Telnet, you must know the target port and if an alternate port has been configured for use. Ports are configured in the answer files used for password management. If multiple systems are on different ports, multiple answer files are required. If using Telnet, passwords cannot be programmatically passed. Answer files must include the management steps and the login process, meaning the Telnet portion of the answer file must be edited.

McAfee ePO

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported for target McAfee ePO instances provided that the connection account has the ability to read from the ORION table.
Authentication	✓	McAfee ePO password changes occur by directly manipulating information in the Orion table or the ePO database, which runs on a Microsoft SQL Server. Access to this database must be available to Privileged Identity. Authentication to a Microsoft SQL Server can be performed using an explicit SQL account (e.g. sa) or a trusted account from the local Windows host or joined directory. When working with a SQL Server from a trusted domain, the account running the console or the scheduling service must be granted the appropriate permissions to the target SQL Server. Or, the SQL Server must permit access with a proper explicit SQL Server account. If attempting to manage a SQL instance on an untrusted host, you are able to use an explicit SQL Server account only.
Password Management	✓	Privileged Identity can manage passwords for target McAfee ePO instances provided the connection account has the the ability to write and update the Orion table.
Ports and Protocols	✓	For most SQL Server installations, including clustered resources, no additional steps are needed. However, SQL Server does allow an SSL-protected connection to be configured. If the connection is enabled for SSL or TLS, management of ePO accounts is no longer possible. By default, SQL Server listens on port 1433, but this port can be configured on a per-IP-address or SQL-instance-basis. Be mindful of any port changes to the SQL server or named instance.

Microsoft Azure Active Directory (AD)

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to Microsoft Azure AD uses an Azure AD account supplied as an email address. The following information is also required: • **Client ID** • **Tenant ID** • **Subscription ID** • **Management Certificate and Certificate Password (Optional)**: Used for discovering systems in the Azure instance
Password Management	✓	Standard AD account management permissions apply.
Ports and Protocols	✓	All management functions occur over an HTTPS connection. If the Privileged Identity host cannot connect directly to the internet, a proxy server connection may need to be configured upon enrollment of the Azure instance.

Note: *If using Microsoft Azure AD as an authentication source for logging into the web application, the application must also be configured in Microsoft Azure AD.*

MySQL

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to a MySQL database can be performed only when using an explicit account. Directory accounts are not supported for management of MySQL databases. MySQL uses a scheme to identify the source of the login account. MySQL instances must be configured with an account allowing access from Privileged Identity host servers. To make a connection, you must know the default database name.
Password Management	✓	
Ports and Protocols	✓	For most MySQL database installations, including clustered resources, no additional steps are needed beyond installing the proper OLE DB provider on the Privileged Identity host performing the management. By default, MySQL listens on port 3306; however, the port can be changed.

Oracle Databases

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to an Oracle database can be performed only when using an explicit account. Directory accounts are not supported for management of Oracle databases.
Password Management	✓	
Ports and Protocols	✓	For most Oracle database installations, including clustered resources, no additional steps are needed beyond installing the proper OLE DB provider on the Privileged Identity host performing the management. By default, Oracle listens on port 1521, but this port can be configured based on service/SID name. Be aware of port changes as well as changes to the names configured in the listeners file on the target Oracle database host. It is helpful to obtain the listener file from the target Oracle database.

Note: *Oracle restricts management of down-level database versions. For more information, please see the Oracle Help Center at https://docs.oracle.com/en/.*

Oracle WebLogic

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported for target WebLogic instances and for accounts found in the core WebLogic product.
Authentication	✓	Authentication to WebLogic instances must use a local WebLogic account.
Password Management	✓	
Ports and Protocols	✓	Ports for WebLogic can vary based on installation and the use of SSL. Without SSL, the default port is 7001. With SSL, the default port is 7002.

Note: *An EAR file must be installed as an enterprise application to start the WebLogic instance.*

OS390

Considerations	Supported	Details
Account Discovery	✗	
Authentication	✓	When establishing an SSH session, authentication to an OS390 host can occur using a certificate or password. Users can originate from a local directory or from a central directory. While all scenarios are supported, each requires different considerations and planning, especially when using certificates. It is important to understand your system's authentication requirements.
Password Management	✓	
Ports and Protocols	✓	If using SSH, take into consideration the requirements for the target SSH port, for encryption, and for HMAC algorithms. If SSH is not used, the 3270 terminal is used instead. 3270 terminal emulation is supported through an add-on component provided by DN-Computing, dn-computing.com. With or without SSL, 3270 terminals run over Telnet. It is important to know which port to use and if SSL is enabled.

SSH and Telnet

Considerations	Supported	Details
Account Discovery	✓	Account discovery for SSH hosts requires the ability to read from **/etc/shadow** and **/etc/password**.
Authentication	✓	When establishing an SSH session, authentication to an SSH host can occur using a certificate or password. Users can originate from a local directory or from a central directory. While all scenarios are supported, each requires different considerations and planning, especially when using certificates. It is important to understand your system's authentication requirements.

Considerations	Supported	Details
Password Management	✓	It is important to know which account will be managed and which account will manage it. It is also important to know the process to follow to perform that management. Management of passwords is performed using answer files.
Ports and Protocols	✓	Modern SSH systems use SSH as the default protocol for management operations. SSH uses a single port, which defaults to TCP 22. If you use Telnet for any reason, the default port is 23, but this can be changed. Whether using SSH or Telnet, you must know the target port and if an alternate port has been configured for use. Ports are configured in the answer files used for password management. If multiple systems are on different ports, multiple answer files are required. If using Telnet, passwords cannot be programmatically passed. Answer files must include the management steps and the login process, meaning the Telnet portion of the answer file must be edited.

> ***Note:*** *Any permission or policy preventing BeyondTrust PI's login account from reading **/etc/shadow** and **/etc/password** will keep enumeration from properly functioning. Also, if the files do not exist in the **/etc** directory, enumeration will not occur.*

> ***Note:*** *Prior to version 5.5.0, BeyondTrust PI would copy **/etc/shadow** and **/etc/password** from the SSH host using SCP to the local PI host for local parsing. Versions after 5.5.0 list the contents of the files within the session, allowing for faster operations. Also, low-powered accounts can use sudo to cat the files, specifically **sudo cat /etc/shadow**.*

PostgreSQL

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to a PostgreSQL database can be performed only when using an explicit account. Directory accounts are not supported for management of PostgreSQL databases. PostgreSQL authentication does not allow remote connections from anywhere out-of-the-box, and rules must be established to allow communications from specific hosts or networks. For the connection to be made, you must know the default database name.
Password Management	✓	
Ports and Protocols	✓	For most PostgreSQL database installations, including clustered resources, no additional steps are needed beyond installing the proper OLE DB provider on the Privileged Identity host performing the management. By default, PostgreSQL listens on port 5432; however, the port can be changed.

Rackspace Public Cloud

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to Rackspace requires using an explicit username and password.
Password Management	✓	
Ports and Protocols	✓	All management functions occur over an HTTPS connection. If the Privileged Identity host cannot connect directly to the internet, a proxy server connection may need to be configured upon enrollment of the Rackspace instance.

Salesforce

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported for Salesforce accounts enrolled with the Chatter service.
Authentication	✓	Authentication to Salesforce uses an account supplied as an email address. An application must be configured in Salesforce to allow connectivity. The Consumer Key and Consumer Secret are required.
Password Management	✓	Privileged Identity can manage passwords for Salesforce accounts provided that the logged in user is permitted to change passwords. Also, the application must allow that sort of management.
Ports and Protocols	✓	All management functions occur over an HTTPS connection. If the Privileged Identity host cannot connect directly to the internet, a proxy server connection may need to be configured upon enrollment of the Salesforce instance.

***Note:** If using Salesforce as an authentication source for logging into the web application, the application must also be configured in Salesforce.*

SAP

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported for target SAP instances and for accounts found in the core SAP product.
Authentication	✓	Authentication to an SAP instance can occur with a local SAP account or a trusted account from another directory. If using a gateway, note the following: • HTTP or non-HTTP • URL path to the server • The NetWeaver add-on must be installed on the gateway host. If a gateway is not used, note the following: • System Number • Client • Destination • Table Name (a default table name is **USERLIST** and column index is **0**.)
Password Management	✓	Privileged Identity can manage passwords for SAP accounts provided that the logged in user is permitted to change passwords. Also, the application must allow that sort of management.
Ports and Protocols	✓	Ports vary based on whether you use the NetWeaver add-on or a direct connection

***Note: Librfc32.dll** must be provided and copied into the **\Windows\system32** directory of the Privileged Identity host managing the SAP instance.*

SoftLayer

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to SoftLayer uses an explicit username and password.
Password Management	✓	
Ports and Protocols	✓	All management functions occur over an HTTPS connection. If the Privileged Identity host cannot connect directly to the internet, a proxy server connection may need to be configured upon enrollment of the SoftLayer instance.

SQL Databases

Considerations	Supported	Details
Account Discovery	✓	Account discovery is supported for target SQL Server instances provided that the connection account has the **Control Server** permission or is a member of the **sysadmin** role.
Authentication	✓	.Authentication to a Microsoft SQL Server can be performed using an explicit SQL account (e.g. sa) or a trusted account from the local Windows host or joined directory. When working with a SQL Server from a trusted domain, the account running the console or the scheduling service must be granted the appropriate permissions to the target SQL Server. Or, the SQL Server must permit access with a proper explicit SQL Server account.If attempting to manage a SQL instance on an untrusted host, you are able to use an explicit SQL Server account only.
Password Management	✓	Privileged Identity can manage passwords for target SQL Server instances provided the connection account has the Control Server server permission or is a member of the sysadmin role.
Ports and Protocols	✓	For most SQL Server installations, including clustered resources, no additional steps are needed. However, SQL Server does allow an SSL-protected connection to be configured. If the connection is enabled for SSL or TLS 1.0, no additional software is needed. If the SQL Server instance is configured to require TLS 1.2, you need to install the latest SQL Server native client on any host managing a SQL Server instance. By default, SQL Server listens on port 1433, but this port can be configured a per-IP-address or SQL-instanc- basis. Be mindful of any port changes to the SQL Server or named instance.

VMware ESX

Considerations	Supported	Details
Account Discovery	✓	
Authentication	✓	Authentication to VMware ESX uses an explicit username and password.
Password Management	✓	
Ports and Protocols	✓	All management functions occur over an HTTPS connection. If the Privileged Identity host cannot connect directly to the internet, a proxy server connection may need to be configured upon enrollment of the VMware ESX instance.

Windows

Considerations	Supported	Details
Account Discovery	✓	Local systems allow administrators to enumerate all accounts on a Windows system. For Active Directory, if you are not an administrator, you may successfully refresh portions of Active Directory for which you have read access. However, a non-fatal error will be received during the refresh. Without administrative rights, you cannot refresh the domain controller system information.
Password Management	✓	When changing a local account password, the change can occur by an administrative account or by the target account changing its own password. When performing an administrative password change, a password reset is actually being performed. When an account is used to change its own password, a change, not a reset, is being performed. When changing a domain account,this change can occur by an administrative account, or by the target account changing its own password, or by a delegated reset.For an account to manage different domain account passwords, the rights required vary based on the domain account.
Ports and Protocols	✓	Windows management occurs via various RPCs and over a range of ports, including port 445, 135, and ephemeral ports. Basic system refreshes and local password management occur over port 445 for all recent versions of Windows. Ephemeral ports are used during account usage discovery and password propagation. The ephemeral port range varies by Windows distribution and can be controlled in the Windows registry. The default ephemeral port range is: • **Windows 2008 and later** = 49152 - 65535 This port range must be accounted for when configuring firewall rules for management of these hosts.

Xerox Phaser Printers

Considerations	Supported	Details
Account Discovery	✗	Account discovery is not supported for Xerox Phaser printers because there is only one account.
Authentication	✓	Authentication to a Xerox Phaser Printer occurs over SNMP via the administrator account. This account can be renamed, which means you must be aware of the current name of this account.
Password Management	✓	Privileged Identity can perform password management for Xerox Phaser printers; however, the administrator accoun tis used to change its own password.
Ports and Protocols	✓	All management operations are performed via SNMP. The default SNMP port is 161. SNMP relies on a community name to aid in authentication. The default community name is public, and the name is subject to change during printer configuration. SNMP with SSL is not supported at this time.