Qualys Integration with CyberArk Application Identity Manager (AIM)

User Guide

February 25, 2019

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Preface

Welcome to Qualys Cloud Platform! In this guide, we'll show you how to use the Qualys integration with CyberArk Application Identity Manager (AIM) for credential management.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

Overview

The Qualys Cloud Based Platform provides an easy way to continuously discover and secure all your global IT assets. With Qualys Cloud Platform you get a single view of your security, compliance and IT posture all in one place - in real time. Qualys Cloud Suite includes a suite of security and compliance applications, built on top of the Qualys Cloud Platform infrastructure and services.

Qualys delivers frequent product updates with new features and improvements leveraging its cloud based infrastructure and services. Click here for the latest Release Notes.

Key Benefits

Using Qualys integration with CyberArk Application Identity Manager, credentials management is simplified as customers no longer need to store and manage their passwords, private keys and certificates within Qualys to perform authenticated scans. This significantly reduces the complexity of credential management because credentials are centrally managed in the CyberArk solution. Organizations can automatically rotate passwords, private keys and certificates based on their security policy, eliminating the need to manually update credentials within the Qualys platform. Further, running credentialed-protected scans yield deeper, more accurate scan results.

Simplified privileged credential management and improved compliance

Internal policies and many regulatory requirements such as those in PCI, SOX, and HIPAA, require full accountability and traceability of all credential use. By storing privileged credentials used by Qualys Vulnerability and Compliance Scanning solution in CyberArk, organizations increase security and can enforce their security policies by automating credential rotation, centrally storing and managing credentials, and fully auditing credential use. Centralized management also makes it easier to update credentials, significantly reducing the potential for human error that can occur when manually maintaining credentials in the Qualys platform.

Facilitates secure scanning, Resulting in better discovery and prioritization

When a trusted scan is performed for vulnerability or compliance assessment, the Qualys scanner logs into the target machine and reads configuration data such as registry values, configuration files/settings, and software inventory details. Qualys uses the configuration data to verify vulnerabilities and make sure configuration settings meet minimum required standards. By leveraging CyberArk automated credential rotation capabilities, which updates and synchronizes privileged account credentials at based on policy, there is never a fear of the Qualys scanner re-using unprotected credentials. This significantly improves security and facilitates wider adoption of credentialed scanning. By leveraging Qualys - CyberArk integration, customers get a better picture of the true state of compliance and vulnerabilities with the added depth of scanning across even the largest environments.

Qualys Integration – How it Works

HOW IT WORKS:

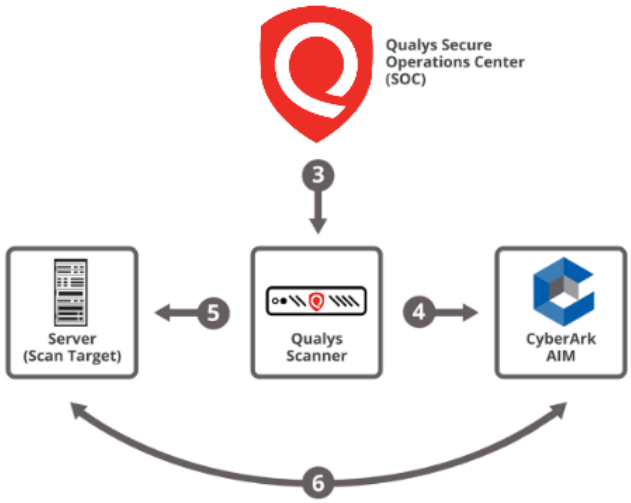


Figure 1: Workflow of the integration between Qualys and CyberArk Application Identity Manager™

BEFORE LAUNCHING THE SCAN

1. User configures the CyberArk solution according to their policies and sets up credentials
2. User configures Qualys to use CyberArk integration by configuring Authentication

LAUNCHING THE SCAN

3. User launches a trusted scan from Qualys
4. The Qualys Scanner Appliance (SA) queries the Central Credential Provider (part of CyberArk Application Identity Manager) for secure credentials retrieval from CyberArk Digital Vault
5. The SA scans the target using the credentials (Windows and Unix)
6. Audit/control/policy enforcement using CyberArk Application Identity Manager

Credential Retrieval

The user launches an authenticated scan on a target machine and the authentication record for the target specifies the CyberArk AIM vault. The service sends a request to the scanner appliance with the CyberArk AIM CCP safe information (application ID, safe name and URL) defined by the customer in the vault record. The appliance uses this information, along with information from the authentication record, to request sensitive information from the vault - the password for a given user name, the private key and/or private key passphrase for a given certificate, the password for root delegation. The information requested depends on the host technology and authentication record settings.

The appliance uses the information retrieved from the vault to log into the target machine and perform the trusted scan. After performing the scan, the scanner appliance deletes every trace of the password and/or private key, and sends the scan results to the Qualys Cloud Platform and these results are available in the user's Qualys account.

How is the integration secured?

It's secured by IP address. The Qualys Application ID configuration Allowed Machines option needs to include IP addresses of the Qualys scanners.

AIM Installation & Configuration

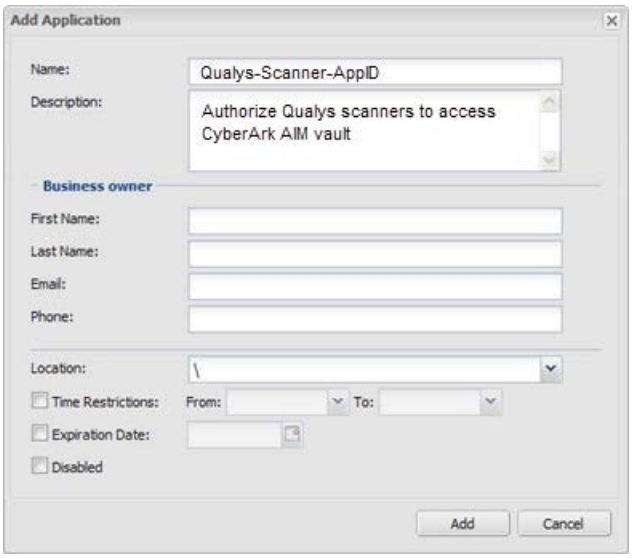
Refer to "Credential Provider and ASCP Implementation Guide" for CyberArk Credential Provider installation. There are no specific steps for configuring AIM Provider with Qualys.

Defining the Application ID (APPID) and Authentication Details

To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

1) Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click Add Application; the Add Application page appears.

Qualys does not have a pre-defined APP ID that the customer must use. One example for defining the Application ID for Qualys scanning would be Qualys-Scanner-AppID.



2) Specify the following information:

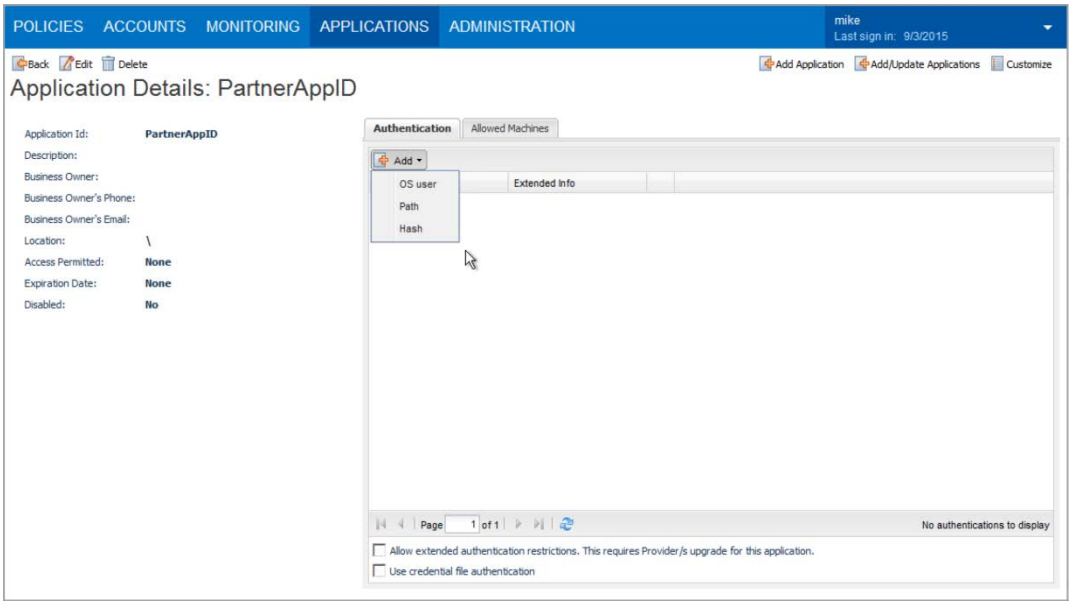
In the Name field, enter the unique name (ID) of the application.
For Qualys, APP ID = Qualys-Scanner-AppID

In the Description field, enter a short description of the application that will help you identify it.

In the Business owner section, specify contact info about the application's Business owner.

In the lowest section, specify the Location of the application in the Vault hierarchy. If a Location is not selected, the application will be added in the same Location as the user who is creating this application.

3) Click Add. The application is added and is displayed in the Application Details page.



4) Please check the box "Allow extended authentication restrictions". This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

5) Specify the application's Authentication details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

On the Authentication tab, click Add. A drop-down list of authentication characteristics appears. Select the authentication characteristic to specify.

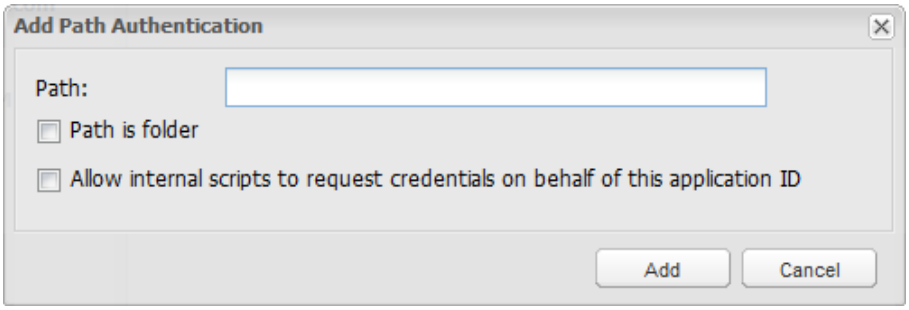
6) Specify the OS user.

Select OS user. The Add Operating System User Authentication window appears.

Specify the name of the OS user who will run the application, then click Add. The OS user is listed in the Authentication tab.

7) Specify the application path.

Select Path. The Add Path Authentication window appears.



Specify the path where the application will run.

- To indicate that the specified path is a folder, select “Path is folder”.

- To allow internal scripts to retrieve the application password for this application, select “Allow internal scripts to request credentials on behalf of this application ID”.

Click Add. The Path is added as an authentication characteristic with the information that you specified.

8) Specify a hash.

Run the AIMGetAppInfo utility to calculate the application’s unique hash. Copy the hash value that is returned by the utility. In the PVWA, select Hash; the Add Hash window appears.

In the Hash field, paste in the application’s unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying ‘#’ after the hash value, followed by the comment.

For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

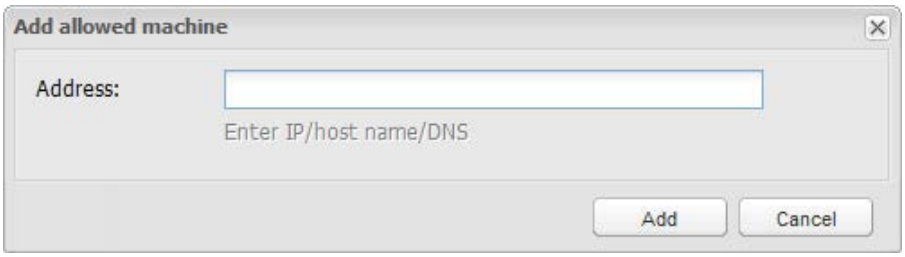
Note: The comment must not include a colon or a semicolon.

Click Add. The Hash is added as an authentication characteristic with the information that you specified.

9) Specify the application’s Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.

Add only the Qualys scanners when defining Allowed Machines. Log into the Qualys UI and go to Help > About to see IP addresses for the Qualys external scanners. Go to Scans > Appliances to get information about the scanner appliances installed in your subscription.

In the Allowed Machines tab, click Add. The Add allowed machine window appears.



Specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click Add. The IP address is listed in the Allowed machines tab.

Make sure the servers allowed include all mid-tier servers or all endpoints where the AIM Credential Providers were installed.

Provisioning Accounts and Setting Permissions for Application Access

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault (Step 1). Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application (Step 2).

1) In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- Manually: Add accounts manually one at a time, and specify all the account details.

- Automatically: Add multiple accounts automatically using the Password Upload feature.

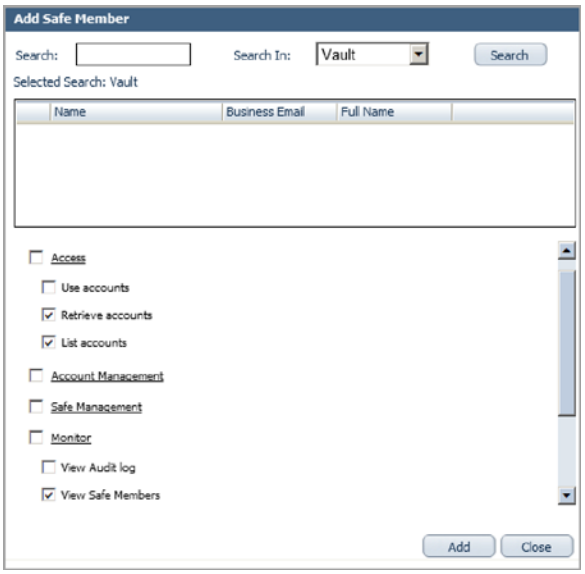
For this step, you require the “Add accounts” authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to the *Privileged Account Security Implementation Guide*.

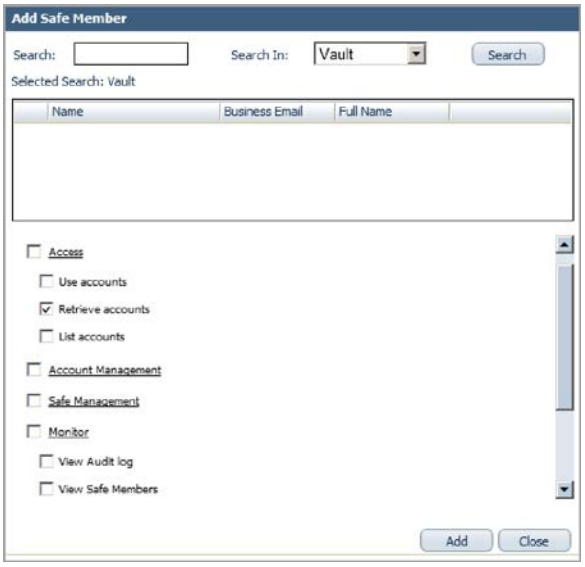
2) Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

Add the Provider user as a Safe Member with the following authorizations:
- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.



Add the application (the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts



If your environment is configured for dual control
In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission: - Access Safe without Confirmation

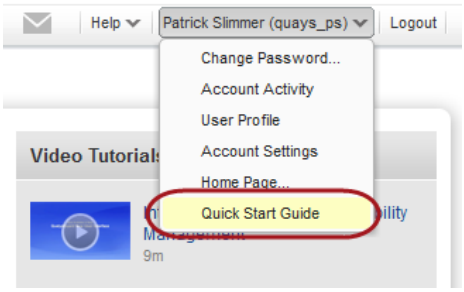
In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.

If the Safe is configured for object level access
Make sure that both the Provider user and the application have access to the password(s) to retrieve. For more information about configuring Safe Members, refer to the *Privileged Account Security Implementation Guide*.

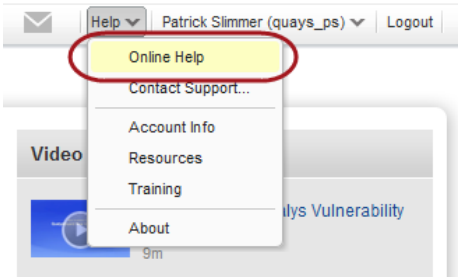
Qualys Configuration

Get Started

The first time you log into Qualys Cloud Platform you'll see our Quick Start Guide which outlines steps for a successful scan. If you don't see this page, you can get to it at any time by selecting Quick Start Guide from the drop-down below your user name (in the top right corner).



Context sensitive online help is available at all times, wherever you are within Qualys Cloud Suite. To get to online help choose Help > Online help from the top menu.



Good to Know – Qualys Cloud Suite implements role based user permissions. The instructions below assume you are the subscription owner with the Manager role. For details on user roles and permissions you can search for "user roles" in the online help.

Steps for authenticated scanning using CyberArk AIM vaults

Step 1 – Add IP Addresses to Scan

Go to Assets > Host Assets to add the IP addresses/ranges you want to scan. We also recommend you organize assets into asset groups and/or apply asset tags. This makes it easier to manage your assets for scanning and reporting.

Asset Groups – Logically group assets by importance, priority, location, ownership, or something else – whatever makes sense for your business. Go to Assets > Asset Groups to get started.

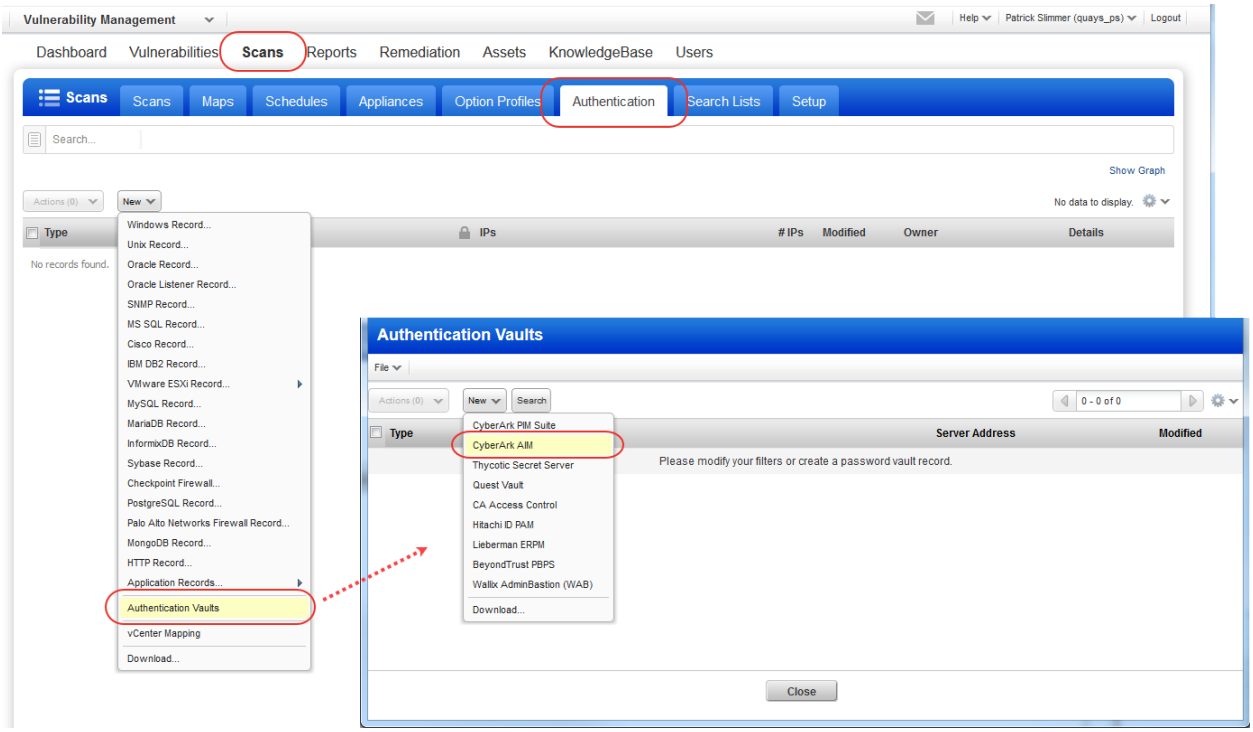
Asset Tags – Automatically discover and organize your assets using tags – this will ensure that your scans and reports are always synchronized with your dynamic business environment. Go to Qualys AssetView to create and manage tags.

Step 2 – Configure Scanner Appliances

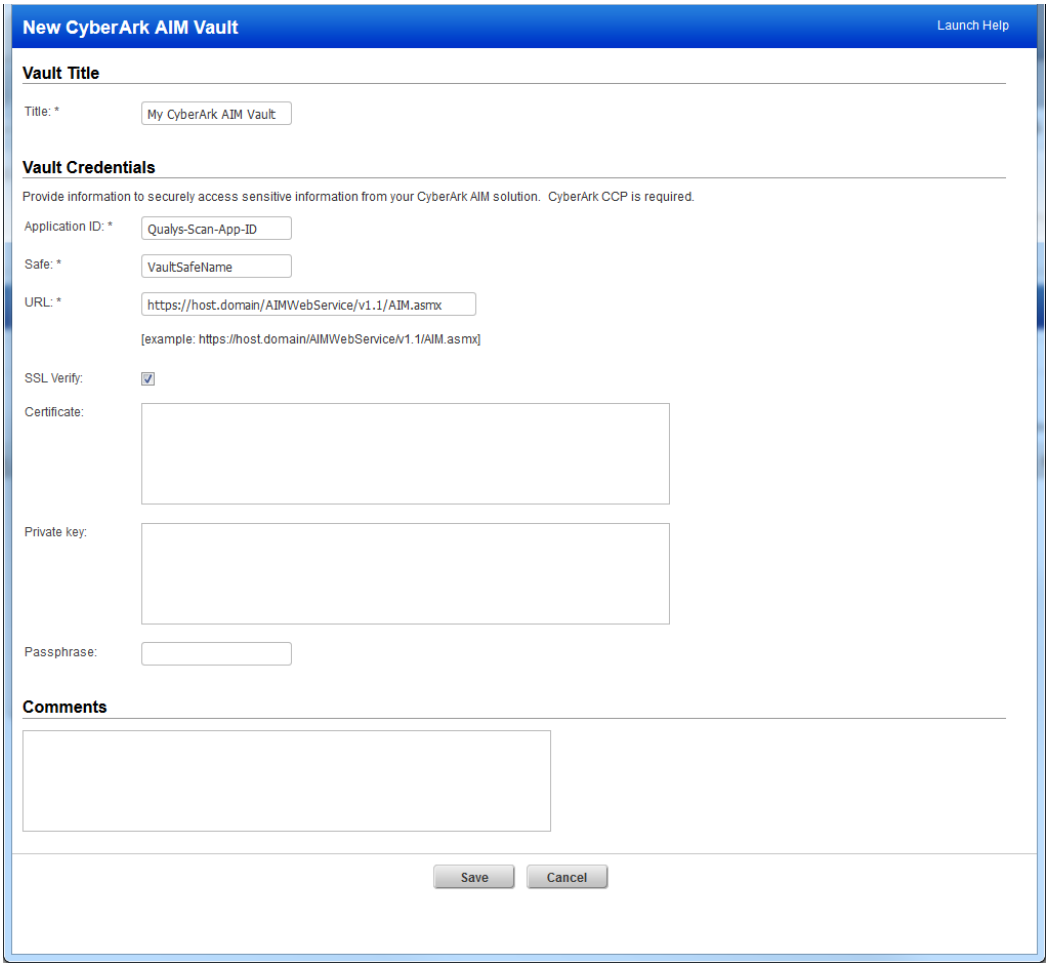
Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Go to Scans > Appliances to add a new appliance and configure it. Want some help? Just go to Help > Online Help and we'll explain all the options.

Step 3 – Configure CyberArk AIM vault records

Go to Scans > Authentication > New > Authentication Vaults. Then choose New > CyberArk AIM.



Provide vault credentials to securely access sensitive information from your CyberArk AIM solution. **CyberArk CCP is required**.



Vault Credentials

Application ID: The application ID name for the CyberArk Central Credential Provider (CCP) web services API. The maximum length is 128 bytes and the first 28 characters must be unique.

- Leading and/or trailing space or periods in the input value will be removed.

- These restricted words cannot be included: Users, Addresses, Areas, XUserRules, unknown, Locations, Safes, Schedule, VaultCategories, Builtin.

- These special characters cannot be included: \ / : * ? " < > | \t \r \n \x1F.

Safe: The name of the digital password safe (max of 28 characters).

- Leading and/or trailing space in the input value will be removed.

- These special characters cannot be included: \ / : * ? " < > | \t \r \n \x1F)

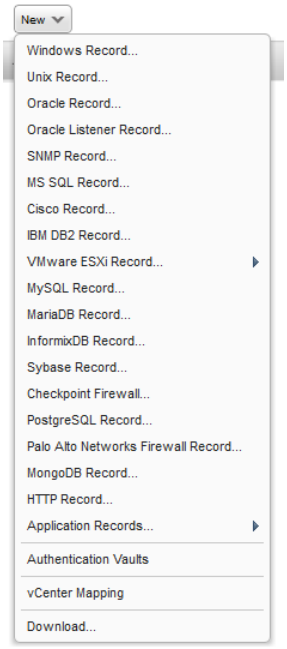
URL: The URL to the CyberArk AIM web service. Choose SSL Verify and we'll verify the server's SSL certificate is valid and trusted. The SSL Verify option is available when the URL uses HTTPS. Sample URL: https://<host.domain>/AIMWebService/v1.1/AIM.asmx

SSL Verify: Qualys scanners will verify the SSL certificate of the web server to make sure the certificate is valid and trusted, unless you clear (un-check) the SSL Verify option. You may want to clear this option to skip SSL verification if the certificate was not issued by a well-known certification authority (CA) or if the certificate is self-signed.

Certificate / Private Key / Passphrase: The certificate and private key/passphrase are required if your server requires a certificate for authentication. Both must be defined together or skipped. The certificate stores the base64-encoded client X.509 certificate in PEM format. The private key stores base64-encoded client private key that corresponds to the public key stored in the certificate.

Step 4 – Configure authentication records

Go to Scans > Authentication > New and choose the authentication type you're interested in. These authentication types can be used in VM and PC: Windows, Unix, Oracle, Oracle Listener, Cisco, IBM DB2, VMware, MySQL, MongoDB, Palo Alto Networks Firewall. These types can be used in PC only: MS SQL, Sybase, Checkpoint Firewall, PostgreSQL, MariaDB.



You can request this sensitive information from your CyberArk AIM solution:

- Login Password (all supported authentication types)
- Private Key & Private Key Passphrase (Unix, PostgreSQL, MongoDB only)
- Root Delegation Password (Unix only)

In the record, you'll provide the name of the Folder and File in the secure digital safe where the password to be used for authentication is stored. You'll also add the IP addresses for the hosts you want to scan with these credentials.

Choose the Authentication Vault option (or Get password from vault: Yes). Then make these selections:

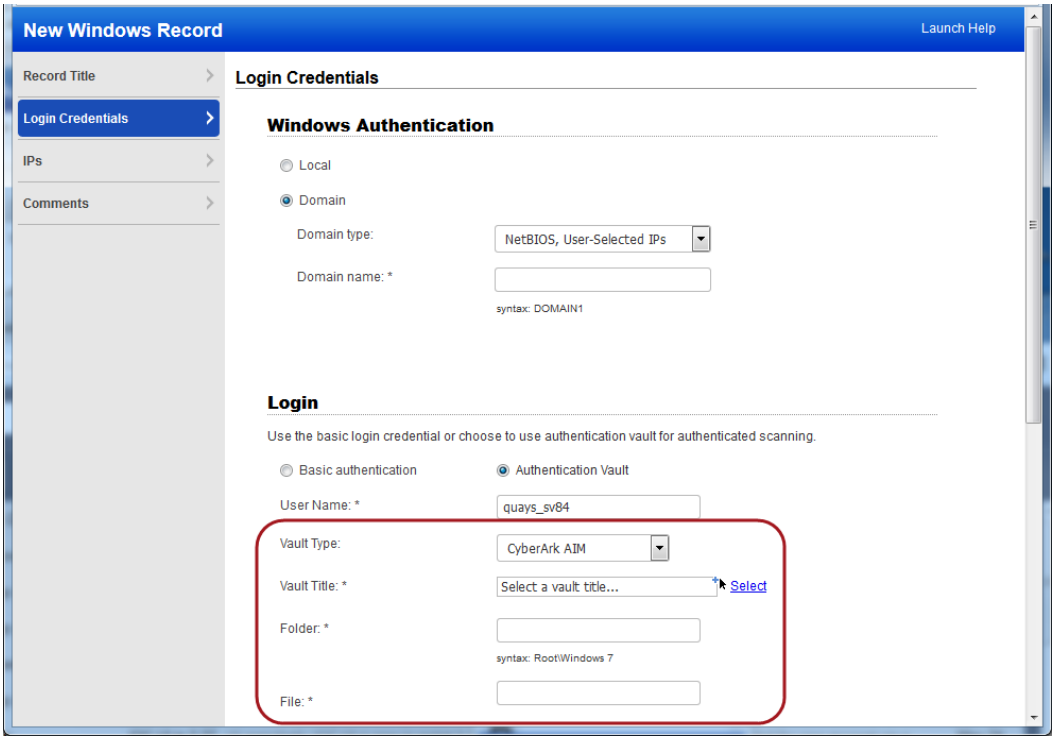
Vault Type: CyberArk AIM

Vault Record / Vault Title: Select the vault record you created in the previous step.

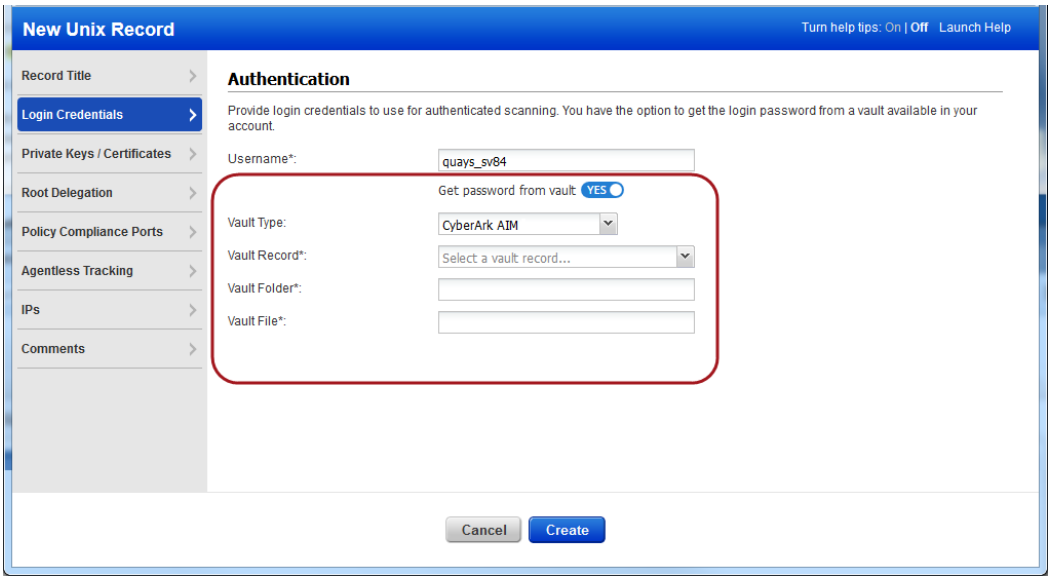
Vault Folder: The vault folder name (169 characters max). Entering a trailing /, as in folder/, is optional (when specified, the service removes the trailing / and does not save it in the folder name). The maximum length of a folder name plus a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included: / : * ? " < > | <tab>

Vault File: The vault filename (165 characters max). The maximum length of a folder name plus a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included: \ / : * ? " < > | <tab>

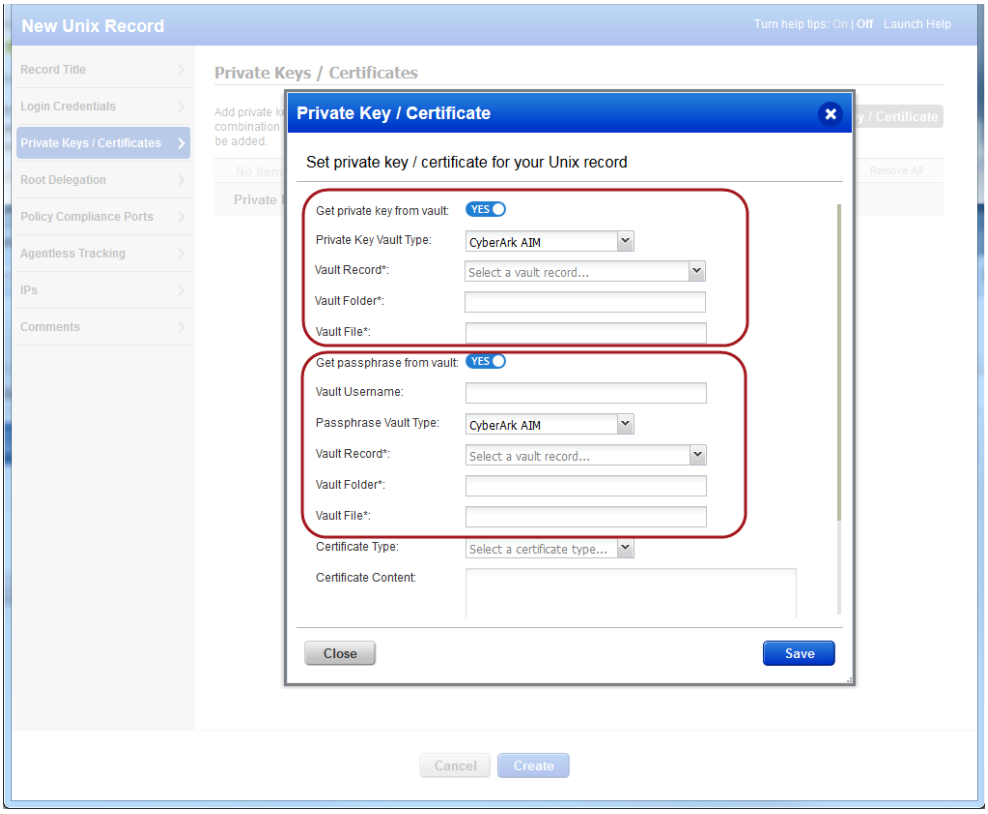
Sample Windows Record: Get password from vault



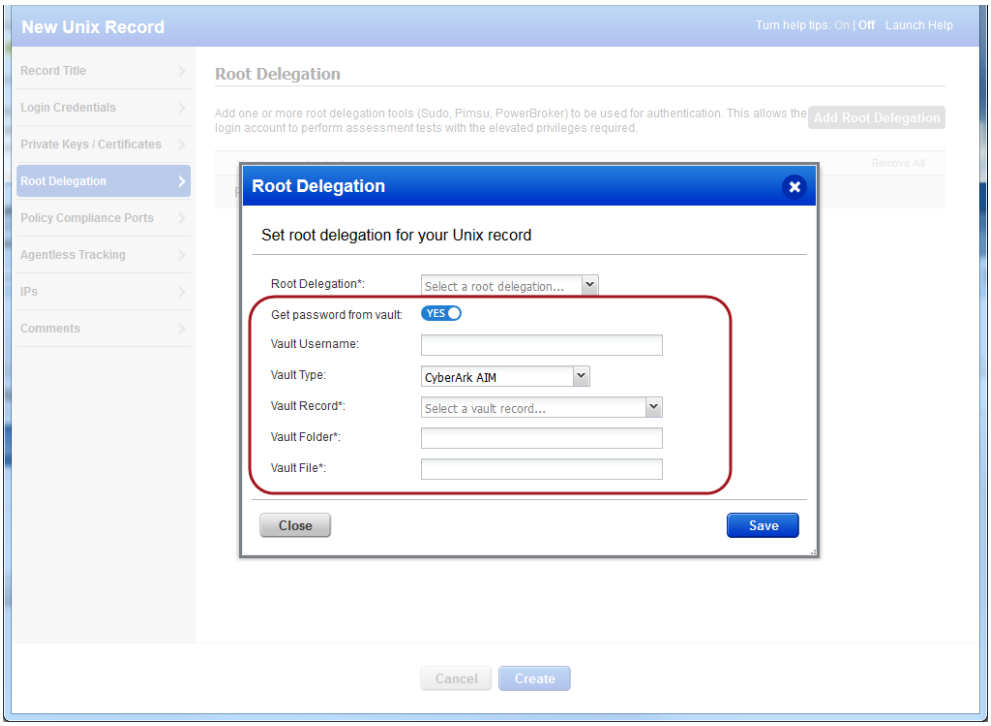
Sample Unix Record: Get password from vault



Sample Unix Record: Get private key from vault and Get passphrase from vault

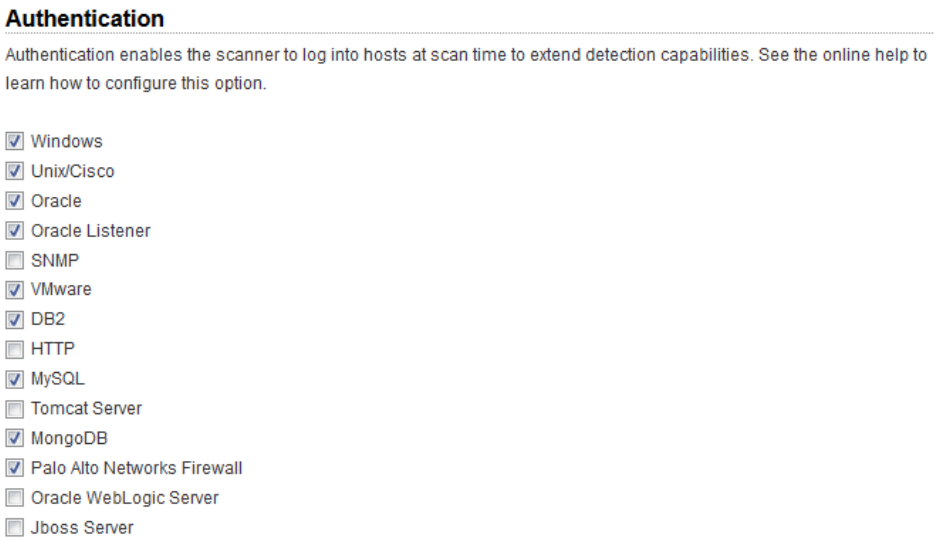


Sample Unix Record: Get password from vault for Root Delegation



Step 5 – Enable authentication for VM scans

Go to VM > Scans > Option Profiles. Create a new option profile or edit an existing one, go to the Scan settings, scroll down to Authentication, and select technologies for the hosts you want to scan.



Step 6 – You're ready to scan!

Go to Scans > New > Scan. Remember online help is always available to help you along the way.

Viewing scan results: For each scan we report authentication status in the Appendix section of the scan results. You'll see hosts that 1) passed authentication, 2) failed authentication, and 3) passed authentication but the login account had insufficient privileges.

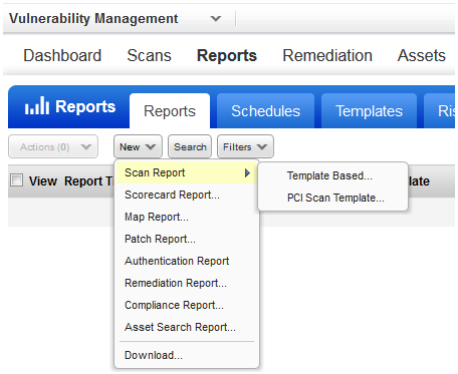
We recommend the Authentication Report: This report tells you the pass/fail status for scanned hosts. If authentication failed on a host then we tell you the cause so you can resolve the issue.

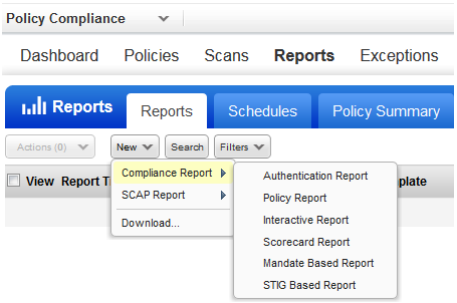
Hosts scanned in VM:
Go to VM > Reports, select New > Authentication Report and run the report.

Hosts scanned in PC:
Go to PC > Reports, select New > Compliance Report > Authentication Report and run the report.
Note - If host authentication fails during a compliance scan we do not perform any control evaluation for the host.

Security and Compliance Reporting

Asset based reports are available in the Reporting section. You can use predefined templates, customize them or create your own. Check out the variety of reports available for VM and PC.





Qualys AssetView gives you a view of all your assets in real time, all in one place. Here you can search your asset inventory in seconds to help you prioritize vulnerabilities and compliance issues. Asset details tell you about each asset including properties and detection information.

Credentials for Common Use Cases

Windows Authentication

What credentials should I use?

Use an account with administrator privileges (local administrator or Windows domain administrator) for the most accurate security assessment and recommended fixes for your system. This allows the scanning engine to collect information based on registry keys, administrative file shares (such as C$) and running services. Less than administrator privileges limits the scan to fewer checks and the results will not be as complete.

Are trust relationships supported?

Yes, we support trust relationships in Windows domain logins. In other words, you can use credentials stored on one domain to authenticate to one or more hosts stored on another domain when trust relationships are present. This is done by the scan targets automatically, using pass-through authentication.

Tell me about Domain settings

If you're using a domain account, enter the domain name and select one of these types in the Windows record:

NetBIOS, User-Selected IPs – When selected we'll use NetBIOS to authenticate to IP addresses in the domain configuration. You enter IPs in the IPs section of the record. A single authentication record may be defined for an entire domain (tree) using this method.

NetBIOS, Service-Selected IPs – When selected we'll use NetBIOS to authenticate to hosts in the domain using credentials stored on the domain. If trust relationships exist and the account's

permissions are properly propagated, it's possible for us to authenticate to hosts which are not members of the same domain.

Active Directory – When selected we'll use an Active Directory forest to authenticate to hosts in a certain domain within the framework. You'll need to enter a Fully Qualified Domain Name (FQDN). If "Follow trust relationships" is selected and trust relationships exist, we'll authenticate to hosts in other domains having a trust relationship with the domain you've defined in the record.

Can I create multiple Windows records?

Yes. You can add as many Windows records as you like. When you have multiple Windows records, we'll try to match each target host to one record. Once a match is found we'll use the matching record for authenticating to the host, and we'll stop looking for other possible matches.

Record types are evaluated in this order

1) Records set to NetBIOS, Service-Selected IPs
2) Records set to NetBIOS, User-Selected IPs
3) Records set to Local
4) Records set to Active Directory

Administrator account vs. another account

First we'll attempt to match the host to a Windows record with an Administrator account following the same order outlined above. If we do match the host to a record with an Administrator account, we'll attempt to match the host to a record with another account, following the same order.

Unix Authentication

What privileges are needed for vulnerability scans?

The account you provide must be able to perform certain commands like 1) execute "uname" to detect the platform for packages, 2) read /etc/redhat-release and execute "rpm" (if the target is running Red Hat), and 3) read /etc/debian_version and execute "dpkg" (if the target is running Debian). There are many more commands that must be performed. The specific commands used for authenticated scanning vary over time as our service is updated. Get a list of commands from our Community.

What privileges are needed for compliance scans?

In order to evaluate all compliance checks you must provide an account with superuser (root) privileges. The compliance scan confirms that full UID=0 access has been granted even if the initial SSH access has been granted to a non-root user. Without full UID=0 access, the scan will not proceed. Note also the account must be configured with the "sh" or "bash" shell. We support use of root delegation tools for systems where remote root login has been disabled for the system to be scanned. However, you cannot use a restricted Unix/Linux account by delegating specific root level commands to the account specified in the sudoers file or equivalent. A non-root account can be used to establish the initial SSH connection but that account must be able to execute a "sudo su –" command (or equivalent) so that account can gain root level (UID=0) access for the compliance scan to proceed.

Using Root Delegation Tools

By enabling root delegation you can provide a lower-privileged user account in the record and still perform scan tests with the elevated privileges of the superuser (root). We support these root delegation tools for authentication: Sudo, Pimsu and PowerBroker. There's an option to get the password for root delegation from your CyberArk AIM vault. Tip - If you have multiple root delegation tools you can order them in your record, and we'll use them in that order.

Using Password Authentication

Under Login Credentials in the record, you can provide a user name and password to be used for login, or you can get your password from a vault configured in your account, like your CyberArk AIM vault.

Skip Password – Select this option if your login account does not have a password

Clear Text Password – The service uses credentials provided in your authentication record for remote access to different command line services such as SSH, telnet and rlogin. The Clear Text Password setting in your record determines whether your credentials may be transmitted in clear text when connecting to services which do not support strong password encryption. For more details you can search for "clear text password" in the online help.

Using Private Keys / Certificates

You can use any combination of private keys (RSA, DSA, ECDSA, ED25519) and certificates (OpenSSH, X.509) for authentication. When you have multiple private keys/certificates you can set the order in your record, and we'll use them in that order.

Private key authentication is supported for SSH2 only. Your private keys can either be unencrypted or encrypted with a passphrase.

You have these options to get key info from a vault:

- Get private key from vault you've configured
- Get private key passphrase from vault you've configured