Unix Authentication

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results and fewer false positives. This document provides tips and best practices for setting up Unix authentication using Qualys Cloud Suite 8.10 or later.

Qualys supports authentication to systems running Unix, Cisco and Checkpoint Firewall.

Few things to know

Why use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? It's required for compliance scans and recommended for vulnerability scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

What are the steps?

First, set up a user account (on target hosts) for authenticated scanning. Then, using Qualys, complete these steps: 1) Add an authentication record to associate credentials with hosts (IPs). We have separate records for Unix, Cisco and Checkpoint Firewall. 2) Launch a scan using an option profile. For a VM scan be sure to enable authentication in the option profile. 3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

Can I have multiple records?

Yes. You can create multiple records with different IP addresses. Each IP address may be included in one Unix type record (Unix Record, Cisco Record or CheckPoint Firewall Record).

Login Credentials

You'll provide us with credentials in authentication records. Many third party vaults are supported. See the Vault Support Matrix in the online help.

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.

Where can I find a list of commands? The article *NIX Authenticated Scan Process and Commands describes the types of commands run, and gives you an idea of the breadth and scope of the commands executed. It includes a list of commands that a Qualys service account might run during a scan. Not every command is run every time, and *nix distributions differ. This list is neither comprehensive nor actively maintained.

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 Sudo or PowerBroker root delegation 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

(Supported for Unix authentication in Unix record settings). These root delegation tools are supported for Unix authentication: Sudo, Pismu, PowerBroker. 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).

Tip - If you have multiple tools you can arrange the tools in a particular order in the record. We'll attempt each root delegation method in sequence, depending on the order configured.

Can I access a password in my password vault?

Yes. We support integration with multiple third party password vaults, including CyberArk PIM Suite, CyberArk AIM, Thycotic Secret Server, Quest Vault, Lieberman ERPM, and more. Go to Scans > Authentication > New > Authentication Vaults and tell us about your vault system. Then choose "Authentication Vault" in your authentication record and select your vault name. At scan time, we'll authenticate to hosts using the account name in your record and the password we find in your vault.

Using private keys

For Unix authentication key authentication is supported for SSH2 only. You can define private keys in Unix authentication records.

Clear Text Password option

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.

Clear Text Password: Not Selected (the default)

Your password will not be transmitted in clear text. The scanning engine only uses strong password encryption for remote login. This setting may prevent the scanning engine from detecting some vulnerabilities on hosts which do not support strong password encryption.

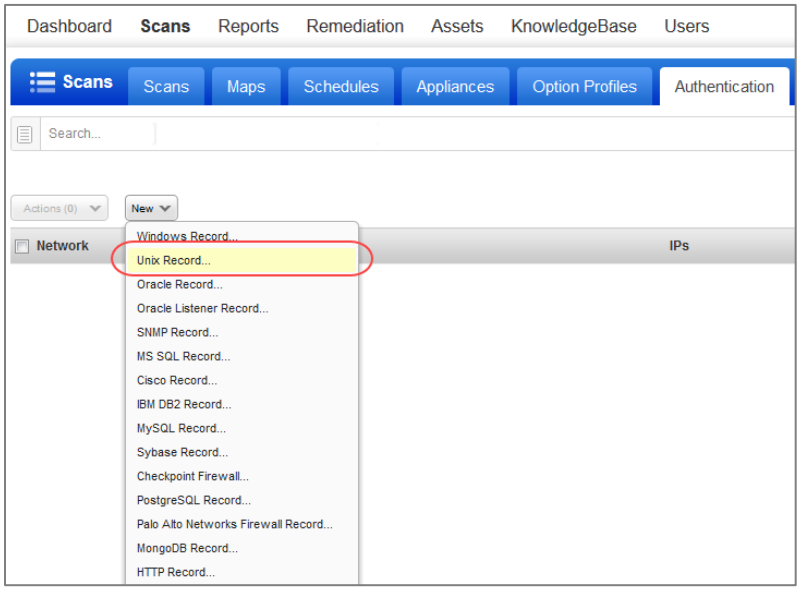
Clear Text Password: Selected

Your password may be transmitted in clear text. The scanning engine uses strong password encryption for remote login, if possible, and falls back to transmitting credentials with weak encryption or in clear text for services which do not support strong password encryption. Important: If these credentials are intercepted by a malicious person, then they may be used to completely compromise a host for attack and theft of information. It is recommended that you replace unsecured services, such as telnet and rlogin, with a secured SSH service. If you must operate unsecured command line services, it is recommended that you operate them within a secured tunnel like SSL/TLS or VPN.

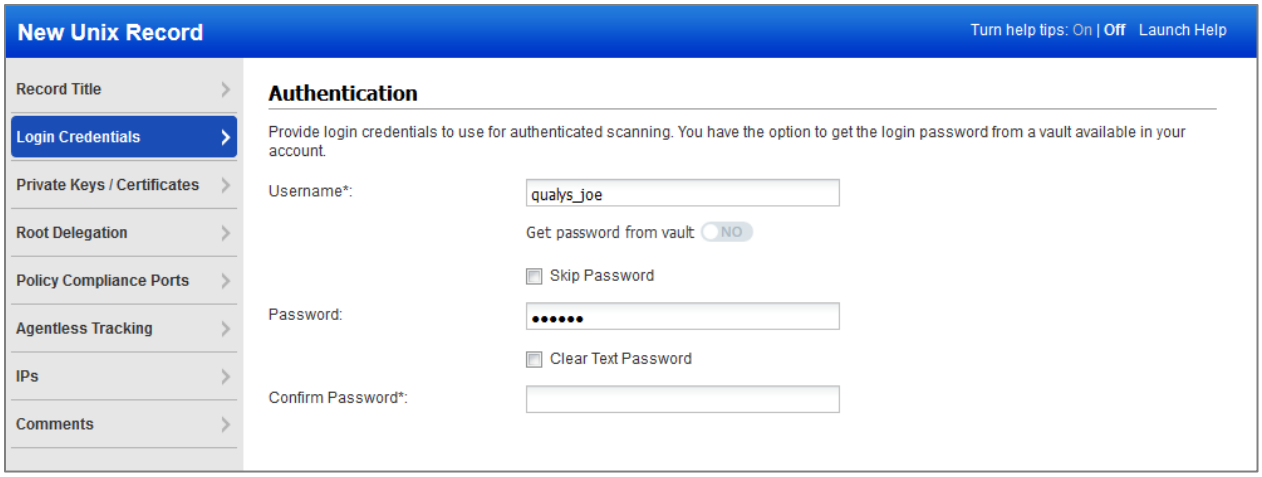
Unix Authentication Record

How to add a Unix record

Go to Scans > Authentication. Then select New > Unix Record. You might be interested in Unix subtypes. You'll see records for Cisco authentication and Checkpoint Firewall authentication.



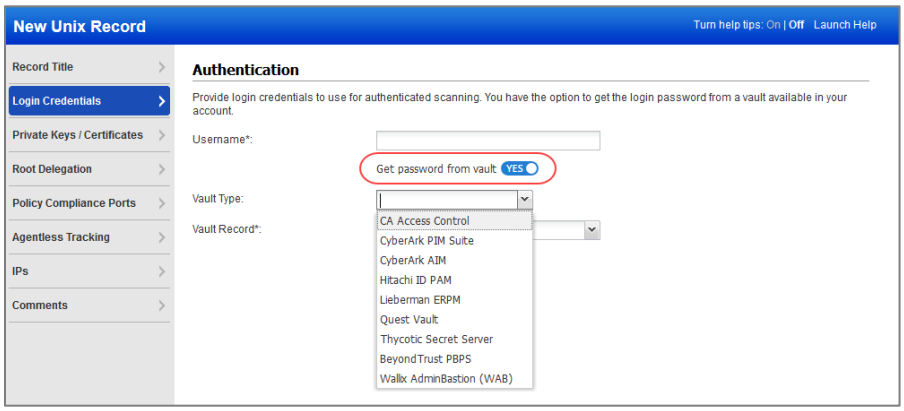
Enter the Unix login credentials (user name, password) our service will use to log in to Unix hosts at scan time. Then walk thru our wizard to select the options you want for private keys, root delegation, policy compliance and target IPs. Our online help is always available to assist you.



Choose options!

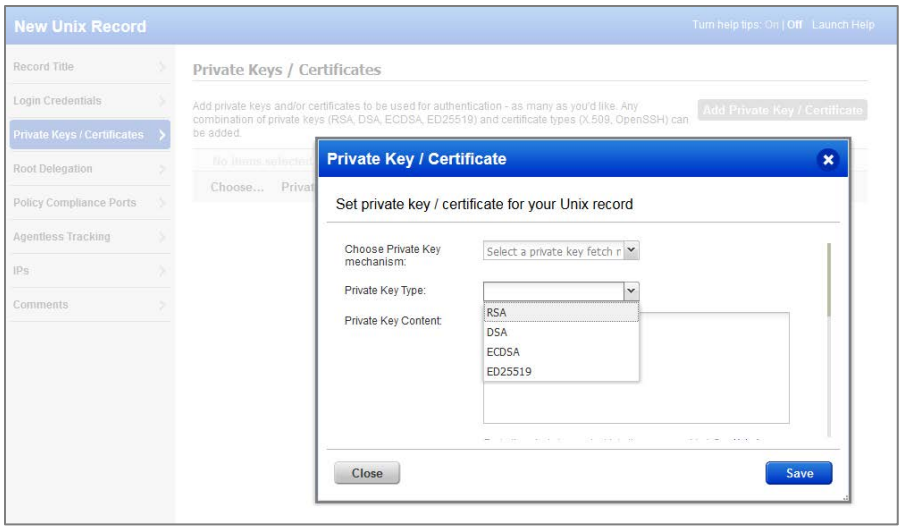
If you provide multiple credentials, authentication is attempted in this order:
1) RSA key, 2) DSA key and then 3) password.

Option to get the password for login credentials from a vault. Choose from vaults available in your account.

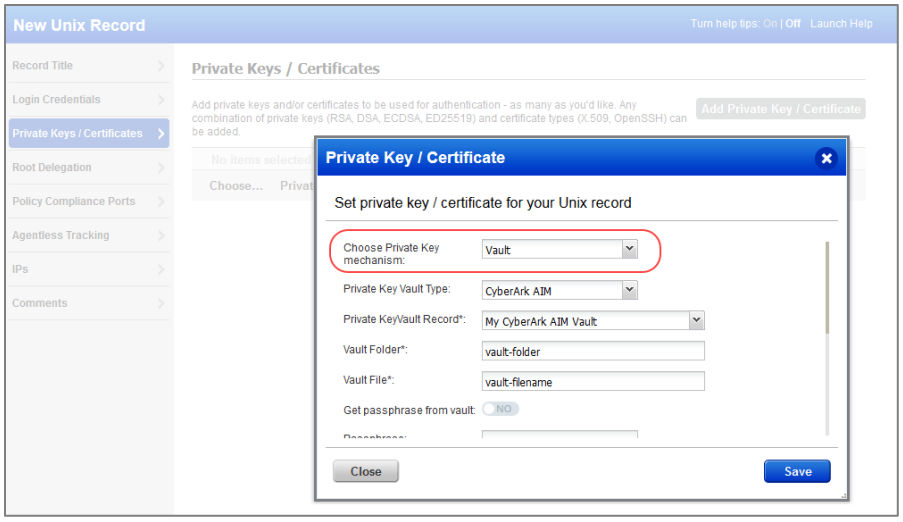


Use any combination of private keys (RSA, DSA, ECDSA, ED25519) and certificates (OpenSSH, X.509) for authentication.

Key authentication is supported for SSH2 only.

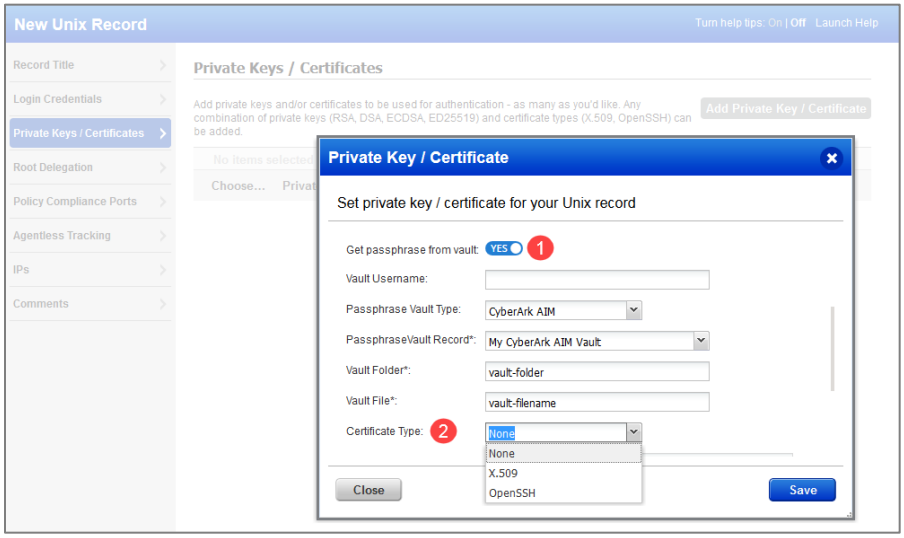


Option to get private key from vault. Choose from vaults available in your account.



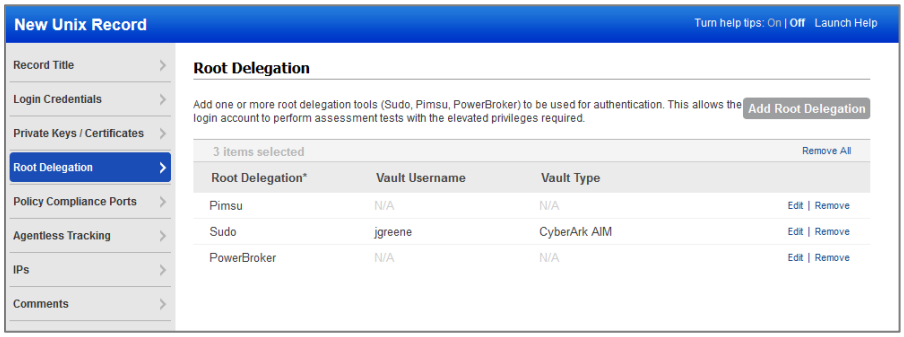
(1) Option to get private key passphrase from vault. Choose from vaults available in your account.

(2) Choose certificate type OpenSSH or X.509.

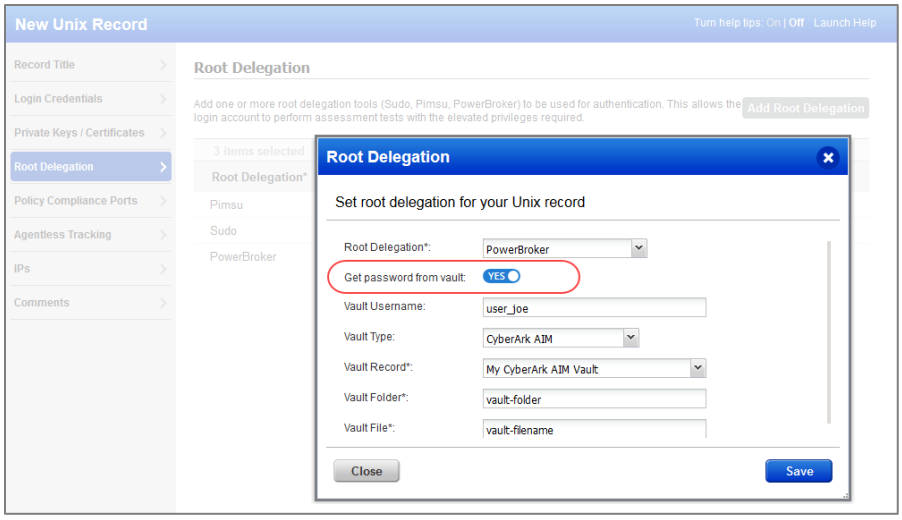


Use multiple root delegation tools - Sudo, Pimsu, PowerBroker.

We'll attempt each root delegation method in sequence, depending on the order configured.



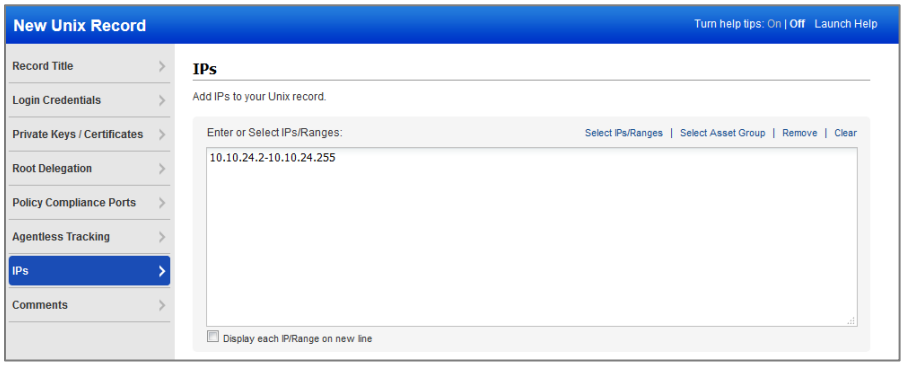
Option to get root delegation password from vault. Choose from vaults available in your account.



Add IPs

Add the IPs you want to scan on the IPs tab.

Each IP may be included in one Unix type record (Unix, Cisco, CheckPoint Firewall).



Ports for compliance scans

The Policy Compliance Ports tab is where you define a custom ports list if services (SSH, telnet, rlogin) are not running on well-known ports for the hosts you will be scanning. By default, these well-known ports are scanned: 22 (SSH), 23 (telnet) and 513 (rlogin). Any one of these services is sufficient for authentication. Good to Know - The actual ports scanned also depends on the Ports setting in the compliance option profile used at scan time.

Using Private Keys / Certificates

For successful authentication, the user account must be added to all target hosts along with the public key, which will be appended to the ".ssh/authorized_keys2" file in the user's home directory. Our service must have full access to the target hosts during scanning. It's possible that manually added options in ".ssh/authorized_keys2" files (like no-pty) lockout our service and in this case security tests cannot be performed. SSH keys and certificates listed below are supported. All of the private keys can either be unencrypted or encrypted with a passphrase.

SSH Private keys

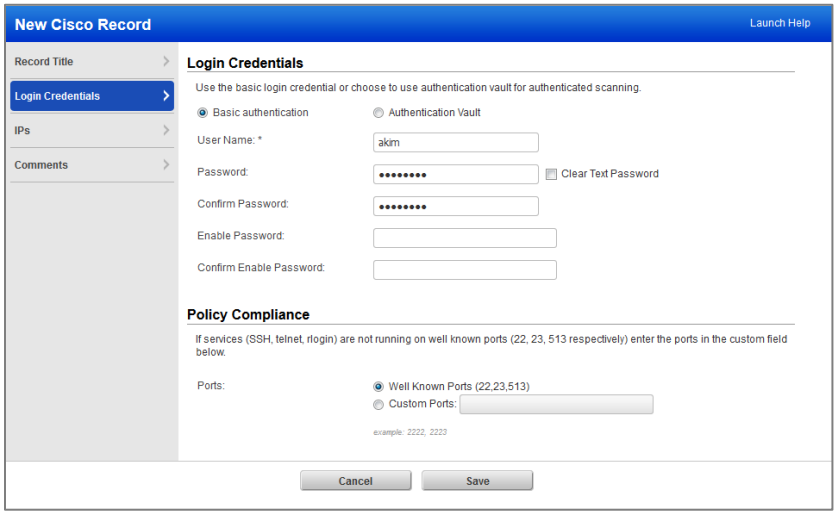
PEM-encoded RSA private key
PEM-encoded DSA private key
PEM-encoded ECDSA private key
OpenSSH-encoded RSA private key

OpenSSH-encoded DSA private key
OpenSSH-encoded ECDSA private key
OpenSSH-encoded EDDSA (currently only ED25519) private key

Supported Certificates

PEM-encoded X.509 certificate using RSA
PEM-encoded X.509 certificate using DSA
PEM-encoded X.509 certificate using ECDSA
OpenSSH certificate using RSA
OpenSSH certificate using DSA
OpenSSH certificate using ECDSA
OpenSSH certificate using EDDSA (currently only ED25519)

Cisco Authentication Record



Which technologies are supported?

Cisco IOS, Cisco ASA, Cisco IOS XE, Cisco NX-OS and Cisco ACS (version 5.8 is not supported)

Which vaults are supported?

CyberArk AIM, CyberArk PIM Suite

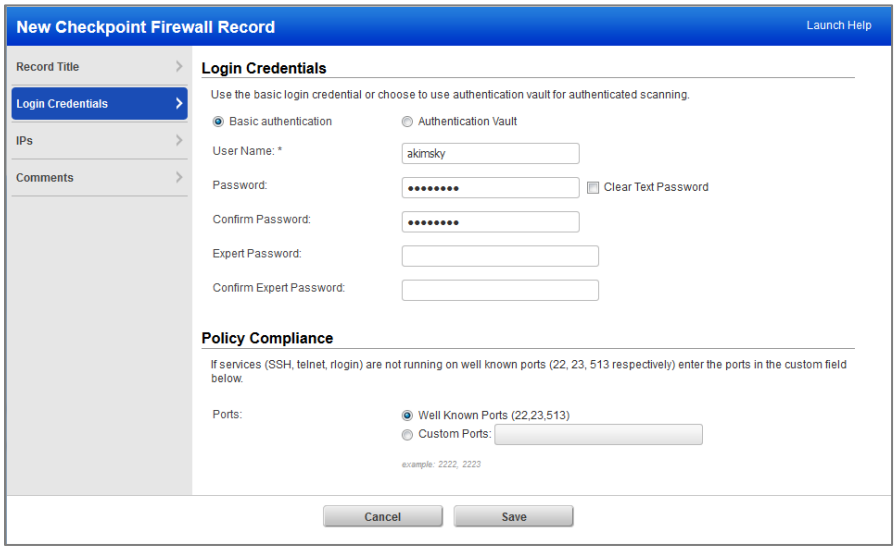
What login credentials are required for Cisco?

1) The user account provided for authentication must have privilege level 15 (equivalent to root level privileges) on the Cisco device in order to perform all checks. You can find a list of commands the account must be able to execute in the online help.

2) We need port 22 (for SSH authentication) or port 23 (for Telnet authentication). If Telnet is the only option for the target you must select the Clear Text Password option in the record since Telnet is an insecure protocol (all information is sent in clear text). We'll use strong password encryption for remote login, if possible, and fall back to transmitting credentials in clear text only when the Clear Text Password option is selected.

3) Your password must not include any spaces.

Checkpoint Firewall Authentication Record



Which technologies are supported?

CheckPoint Gaia and SecurePlatform PRO operating systems:
- CheckPoint Gaia R75-R77
- CheckPoint SecurePlatform PRO R75-77

Which vaults are supported?

CyberArk AIM, CyberArk PIM Suite

What login credentials are required for Checkpoint Firewall?

1) The user account you provide for authentication must have administrative level privileges on the Checkpoint device to perform all checks, and must be able to execute these commands:

```
ver
expert (to switch to expert mode)
cpstat os
```

2) TCP port 22 must be open on the scan target for SSH authentication.

3) Your password must not include any spaces.

Tell me about the Expert Password option

If the “expert” command on the target host requires a password, then you must also provide the expert password in the record. (Note: The pooled credentials feature is not supported if the "expert" command requires a password and the password is specified.)

Last updated: April 30, 2019