

VMware 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 VMware authentication.

A few things to consider

Why should I 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.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

[Authentication Technologies Matrix](#)

What are the steps?

First, set up a VMware user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys, complete these steps: 1) Add a VMware authentication record to associate credentials with hosts. 2) Launch a scan using an option profile with authentication enabled (it's always enabled in compliance profiles). 3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

What's supported?

You can perform authenticated mapping and scanning of VMware vSphere components running VMware ESXi 4.x, 5.x and 6.x, and ESX 3.5 and above. VMware authentication is supported for maps, vulnerability scans and compliance scans. For authenticated maps, the discovery includes only ESXi hosts and the map results identify detected ESXi servers and their guest systems.

What credentials should I use?

You'll need to provide a service credential with at least Read-Only access to your ESXi hosts. Certain additional privileges are also required: Global.Settings, Host.Config.Change settings and Authorization.ModifyPermissions (ESXi 6.5 and 6.0). See the help to learn how to create a role with these required privileges.

Are your ESXi hosts joined to an Active Directory domain? If yes, then a Domain-level credential can be used. If not, then an individual credential on each target machine is required.

Note:

We use SOAP API's for VMware ESXi and Vcenter scanning.

The following table provides examples of different scans and the credentials to be used in each case:

Type of Scan	Credentials to be Used
Full vulnerability VM scan for VMware ESXi or vCenter	Read-only credentials
Basic compliance scan for VMware ESXi or vCenter	Elevated credentials
Indirect scanning (scanning ESXi's through vCenter)	Admin credentials (as we need to enumerate VMware ESXi's that exist in Vcenter)

Tell me about authenticated maps

If you run a map using VMware authentication, we'll use a vSphere API call to retrieve a list of virtual guest hosts residing on a VMware server. Only running virtual guests will be enumerated by the vSphere API and shown in your map results. Note only virtual guests that have VMware Tools installed appear in map results.

Communications with VMware

We establish communication against the vSphere API/VI API (port 443 by default) which is provided by each ESXi host. The vSphere API is a SOAP API used by all vSphere components. This is the same API the VI Client uses to communicate with ESXi hosts. Routing and firewalls between scanner appliances and this API must allow this communication.

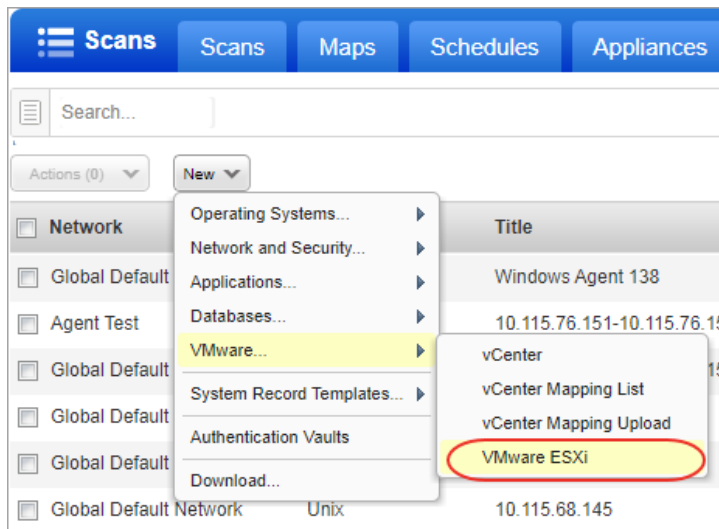
Our service does not currently communicate with/through vCenter Server.

VMware Authentication Records

You'll create VMware authentication records in Qualys to associate credentials with hosts.

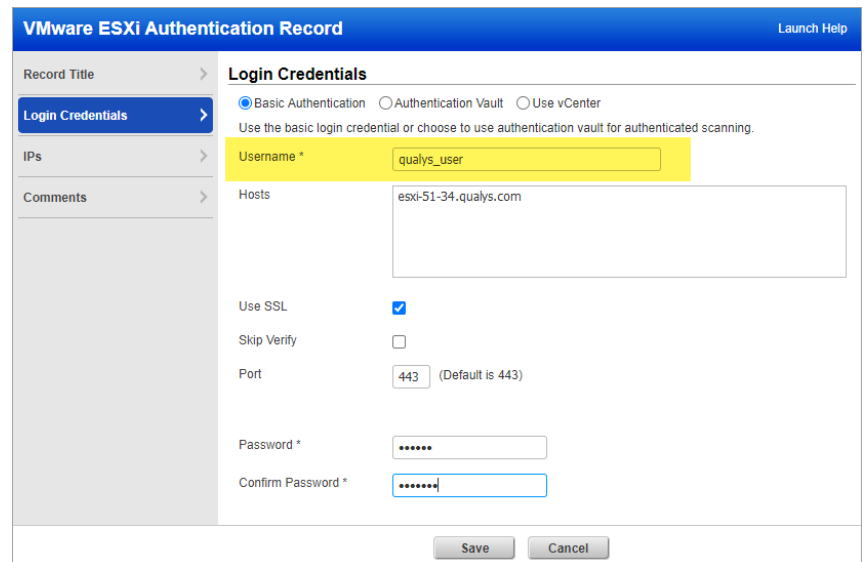
Where do I create records?

Go to Scans > Authentication > New > VMware > VMware ESXi.



Which user name do I enter?

Enter an ESXi user name or a Windows domain user name in the format domain\username.



VMware ESXi Authentication Record Launch Help

Record Title > **Login Credentials**

☒ Basic Authentication ☐ Authentication Vault ☐ Use vCenter

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Username *

Hosts

Use SSL ☒

Skip Verify ☐

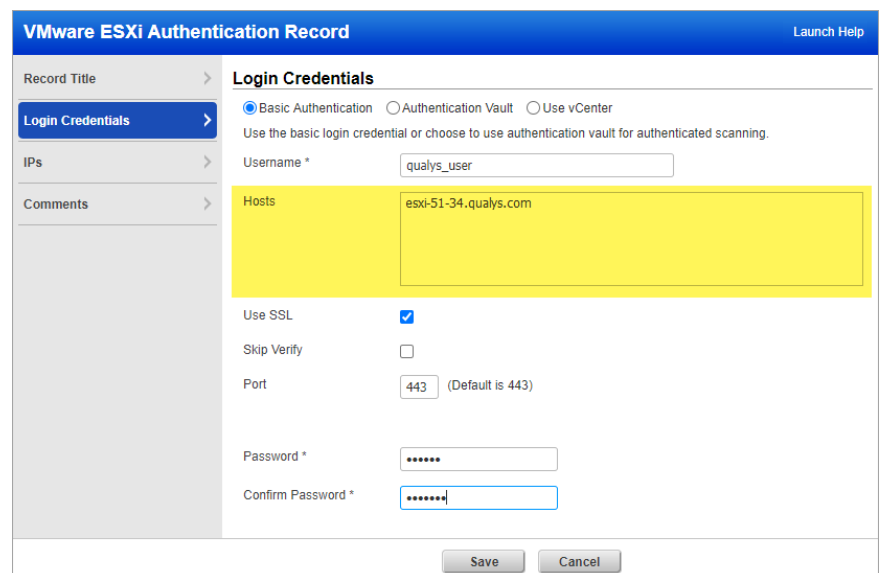
Port (Default is 443)

Password *

Confirm Password *

What do I enter in the Hosts field?

Provide a list of FQDNs for the hosts that correspond to all ESXi host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.



VMware ESXi Authentication Record Launch Help

Record Title > **Login Credentials**

☒ Basic Authentication ☐ Authentication Vault ☐ Use vCenter

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Username *

Hosts

Use SSL ☒

Skip Verify ☐

Port (Default is 443)

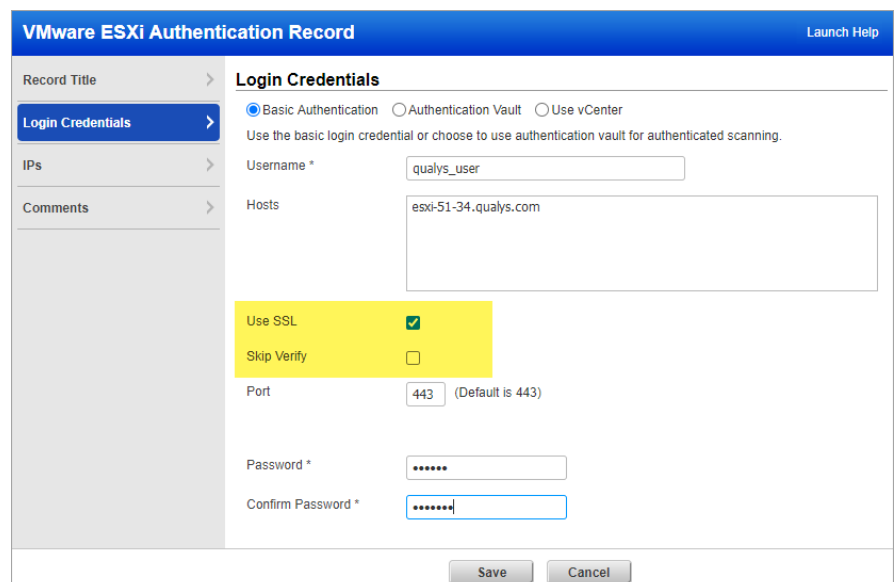
Password *

Confirm Password *

Certificate validation options

Select the “Use SSL” option for a complete SSL certificate validation.

Select “Skip Verify” if the host SSL certificate is self-signed or uses an SSL certificate signed by a custom root CA. A list of host FQDNs is not required in this case.



VMware ESXi Authentication Record Launch Help

Record Title > **Login Credentials**

☒ Basic Authentication ☐ Authentication Vault ☐ Use vCenter

Use the basic login credential or choose to use authentication vault for authenticated scanning.

Username *

Hosts

Use SSL ☒

Skip Verify ☐

Port (Default is 443)

Password *

Confirm Password *

Tell me about the Port setting

By default the service communicates with ESXi web services on port 443. This can be customized.

The screenshot shows the 'Login Credentials' tab of the 'VMware ESXi Authentication Record' form. The 'Basic Authentication' radio button is selected. The 'Username' field contains 'qualys_user' and the 'Hosts' field contains 'esxi-51-34.qualys.com'. The 'Port' field is highlighted in yellow and contains '443' with '(Default is 443)' next to it. The 'Use SSL' checkbox is checked, and 'Skip Verify' is unchecked. The 'Password' and 'Confirm Password' fields are masked with asterisks. 'Save' and 'Cancel' buttons are at the bottom right.

Can I access a password in a vault?

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

This screenshot shows the 'Authentication Vault' radio button selected. The 'Vault Type' dropdown menu is open, showing options like 'CyberArk PIM Suite', 'Thycotic Secret Server', 'Quest Server', 'CA Access Control', 'Lieberman ERPM', 'CyberArk AIM', and 'BeyondTrust PBPS'. The 'Vault Title' field is highlighted in yellow and contains a 'Select' button. The 'Folder' and 'File' fields are also highlighted in yellow. 'Save' and 'Cancel' buttons are at the bottom right.

Which IPs do I add to my record?

Add the IP addresses for the ESXi servers that the scanning engine should log into using the specified credentials. Note you can add one particular ESXi server to only one VMware record in your account.

The screenshot shows the 'IPs' tab of the 'VMware ESXi Authentication Record' form. It prompts the user to 'Add IPs to your VMware ESXi record.' and provides a text area to 'Enter or Select IPs'. The IP '10.10.34.196' is entered. Above the text area are links for 'Select IPs', 'Select Asset Group', 'Remove', and 'Clear'. A checkbox for 'Display each IP/Range on new line' is at the bottom left. 'Save' and 'Cancel' buttons are at the bottom right.

Last updated: February 27, 2023