Tenable and VMware Integration Guide

Last Revised: November 19, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable for VMware **4**

Overview 4

How It Works 5

API Call Pattern 6

What Information Does the VMware Integration Collect? **7**

What the VMware Integration Does Not Collect 7

Integration Limitations **9**

Configure the VMware Integration with Tenable One Vulnerability Management **10**

Required Permissions 10

Scan Configuration – VMware vCenter API 12

Scan Configuration – VMware ESX SOAP API 15

Configure the VMware Integration with Tenable Nessus **17**

Required Permissions 17

Scan Configuration – VMware vCenter API 19

Scan Configuration – VMware ESX SOAP API 21

Configure VMware vCenter API integration with Tenable Security Center **24**

Required Permissions 24

Scan Configuration – VMware vCenter API 25

Auto-Discovery of ESXi Hosts and Virtual Machines **29**

Compliance **31**

Scan Results Review **32**

Plugin families and plugins 32

Debug Log Reporting **35**

Additional Information **37**

Helpful Tips 37

Testing Integration Connectivity 38

vCenter API authentication 38

List the ESXi hosts vCenter manages 39

List installed software components (VIBs) per ESXi host 40

List virtual machines on one ESXi host 42

Retrieve details for a specific virtual machine 42

Frequently Asked Questions **44**

Welcome to Tenable for VMware

This document provides information and steps for integrating Tenable One Vulnerability Management, Tenable Nessus, or Tenable Security Center with VMware vSphere (vCenter Server and ESXi). For more information, refer to the following product documentation:

- Tenable One Vulnerability Management
- Tenable Security Center
- Tenable Nessus

Overview

Virtualization environments combine hypervisors, management servers, and often a very large number of virtual machines. Integrating Tenable One Vulnerability Management, Tenable Security Center, or Tenable Nessus with VMware allows you to assess these environments without maintaining hand-built target lists.

The integration collects information from vCenter servers, ESXi servers, or a combination of both. You integrate with VMware by listing VMware ESXi and/or vCenter servers as scan targets. Additional functionality becomes available when you enable credentialed scans using the **VMware vCenter API** and **VMware ESX SOAP API** credentials for the respective hosts. Together, these capabilities deliver a complete perspective of cyber exposure across the virtual environment:

- **Host enumeration** – discover the ESXi hosts a vCenter server manages, including hosts that are not directly routable from the scanner.
- **Virtual machine identification** – enumerate active (powered on) and inactive (powered off) virtual machines per ESXi host.
- **Software version tracking** – collect ESXi and vCenter versions, and collect VMware Installation Bundles (VIBs) for each managed ESXi host.

- **Configuration insight from the management tier** – run compliance/audit checks against vCenter and ESXi configuration.

The integration supports Tenable One Vulnerability Management, Tenable Nessus, and Tenable Security Center. For details on VMware's own APIs, permission models, and product versions, refer to VMware's official documentation.

How It Works

A vCenter server manages one or more ESXi hosts, and each ESXi host runs one or more virtual machines. Tenable authenticates to the management tier (vCenter) or directly to a hypervisor (ESXi) and works down that hierarchy.

- **API support**: the **VMware vCenter API** credential supports both a SOAP API and a REST API. Tenable automatically selects which API to use based on the detected vCenter/ESXi version – the **SOAP API for versions earlier than 7.0.3** and the **REST API for version 7.0.3 and later**.
- **Compliance scanning**: compliance scanning always uses the SOAP API, regardless of version, because it collects configuration data at a level of detail the REST API does not expose.
- **Connection targets**: the integration can connect directly to a single ESXi hypervisor (using the **VMware ESX SOAP API** credential), directly to a vCenter management server (using the **VMware vCenter API** credential), or to both in the same scan.
- **Credential inheritance**: credentials entered for a vCenter server apply to the ESXi hosts and virtual machines that vCenter manages for the purposes of management-tier data collection – you do not need separate ESXi credentials to collect version data, VIBs, or VM inventory for vCenter-managed hosts. Standalone ESXi hosts that vCenter does not manage require their own VMware ESX SOAP API credential.
- **Host-level and guest-level data requires additional credentials**: the VMware credentials do not authenticate to the underlying operating systems. To assess the vCenter appliance OS, an ESXi host OS, or a guest OS inside a virtual machine, add a separate SSH or Windows credential targeting that host.

Caution: Tenable does not support mixed-version environments where the REST API is unavailable on some hosts. For example, vCenter 7.0.3 managing ESXi servers earlier than 7.0.3 is **not** supported, but vCenter 8 managing ESXi 7.0.3 is supported.

API Call Pattern

This is not a per-target secret-retrieval integration. Data collection is centralized — Tenable executes collection against a single target in the scan and reuses the stored results to report on the other targets enumerated during the scan. Per scan, the REST API request pattern against vCenter is:

1. POST /api/session — authenticate and obtain a session token (once).
2. GET /api/vcenter/host — list the ESXi hosts vCenter manages (once).
3. GET /api/esx/hosts/<host>/software/installed-components — retrieve installed software components (VIBs), once per managed ESXi host.
4. GET /api/vcenter/vm?hosts=<host> — list virtual machines, once per managed ESXi host.
5. GET /api/vcenter/vm/<vm>/guest/identity — retrieve virtual machine details, once per virtual machine. For powered-off VMs this returns `503 Service Unavailable` and the integration falls back to GET /api/vcenter/vm/<vm>.

Request volume therefore scales with the number of managed hosts and virtual machines rather than with the number of scan targets. Disabling **Report Active and Inactive Virtual Machines** removes steps 4 and 5 and materially reduces the number of requests the scanner makes.

Caution: The standard "credentialed checks" concept does not apply here the way it does for a traditional SSH or Windows scan. Tenable authenticates to the vCenter or ESXi *API*, not to the host operating system. Unless an SSH credential is also included, **Credentialed Checks: yes/no** in plugin 19506 (Nessus Scan Information) does not represent successful or failed authentication to the host. Instead: **yes** means the integration collected VIBs for that host and **no** means it did not. Additionally, when scanning vCenter-managed ESXi hosts with API credentials, the vCenter host's own results always show **Credentialed Checks: No** — verify authentication by checking the ESXi hosts' results instead.

What Information Does the VMware Integration Collect?

> **Note**: The Tenable VMware integration supports both IPv4 and IPv6 environments.

ESXi and vCenter versions

The majority of VMware vulnerability checks are based on the versions of ESXi and/or vCenter. Scans collect the versions of both ESXi and vCenter servers in the target list through an *unauthenticated* API call. Where a vCenter server manages one or more ESXi servers, ESXi version information can also be obtained from the vCenter server – useful when ESXi servers are not routable from the scanner. This path requires successful authentication to the vCenter server.

VMware Installation Bundles (VIBs)

In addition to version information, credentialed scans collect VMware Installation Bundles. Collecting VIBs requires successful authentication to vCenter or ESXi, and in the case of vCenter it also requires Lifecycle Manager permissions (see Required permissions). Collected VIBs are stored in the scanner's Knowledge Base (KB) and are used by the VMware ESX Local Security Checks plugin family. Successful collection of VIBs is the criterion by which an ESXi host may have **Credentialed Checks** set to **yes**. Any credential you configure for vCenter or ESXi hosts must be able to list VIBs.

Managed ESXi hosts and virtual machine inventory

With a vCenter credential, the integration enumerates the ESXi hosts vCenter manages and the virtual machines residing on each host, reporting active (powered on) and inactive (powered off) virtual machines against the applicable ESXi host. When **Auto-Discovery** is enabled, these enumerated ESXi hosts and virtual machines are also added to the scan as additional targets – see **Auto-Discovery of ESXi hosts and virtual machines**.

What the VMware Integration Does Not Collect

- The integration does not collect information about the **vCenter or ESXi host operating systems**.
- The integration cannot collect full information about the **guest operating systems running inside virtual machines** (for example, guest OS patch level and installed software).
- Tenable does not run vulnerability detections against the specific VIB data collected. VIB data supports version-based detections and credentialed-check status.

Note: To assess the vCenter server operating system, configure an additional SSH or Windows credential for the vCenter server. For ESXi hosts, an additional SSH credential is also an alternate method of collecting VIBs. For virtual machines discovered through the integration, configure additional SSH or Windows credentials against each guest operating system you want to assess.

Integration Limitations

- **Compliance and Auto-Discovery are mutually exclusive.** Compliance scanning is unavailable when the Auto-Discovery feature is enabled.
- **Auto-Discovery requires vCenter/ESXi 7.0.3 or later**, and requires a vCenter credential (it is not available with an ESXi-only credential).
- **Mixed-version environments are unsupported** where the REST API is not available on all hosts (for example, vCenter 7.0.3 managing ESXi earlier than 7.0.3).
- **Scanner topology constraint.** Tenable recommends using a scanner group containing a single scanner with Auto-Discovery credentials, and entering only a single initial host in the scan. Multiple scanners in an Auto-Discovery scan can cause discovered targets to be scanned more than once.
- **Plugin family dependency.** ESXi vulnerability detection plugins belong to the VMware ESX Local Security Checks plugin family. If that family is disabled, scan results do not include those detections.

VMware vCenter support matrix

Feature	Requires Authentication	Supported vCenter Version
Vulnerability Management	No	7.x, 8.x, 9.x
Auto-Discovery	Yes	7.0.3+, 8.x, 9.x
Audit / Compliance	Yes	6.x, 7.x, 8.x, 9.x
VIB Enumeration	Yes	7.0.3+, 8.x, 9.x
Active / Inactive VMs	Yes	7.0.3+, 8.x, 9.x

Configure the VMware Integration with Tenable One Vulnerability Management

Required User Role: Scan Operator, Standard User, Scan Manager, or Administrator.

Required Scan Permissions: Can Scan.

Tenable One Vulnerability Management exposes two VMware credentials in the **Miscellaneous** credential category:

- **VMware vCenter API** – for vCenter servers and the ESXi hosts and virtual machines they manage. Supports vCenter 6.x through 9.x. Uses the REST API on 7.0.3+ and the SOAP API on earlier versions.
- **VMware ESX SOAP API** – for authentication directly to targeted ESXi hosts to collect VIBs and virtual machine inventory.

Required Permissions

Within VMware, the minimum privileges depend on which API the scan uses.

Scan Type	API Type	Permissions Needed
vCenter credential for vulnerability scanning (7.0.3+)	REST	vCenter account with read permissions, plus VMware vSphere Lifecycle Manager: Image Privileges = Read
vCenter credential for vulnerability scanning (earlier than 7.0.3)	SOAP	vCenter admin account with read and write permissions
Standalone ESXi hosts using	SOAP	User = Read Only (or administrator)

ESXi credentials		
Compliance scan	SOAP	Global → Settings

To create a minimally privileged vCenter user role:

1. Log in to vCenter.
2. (Optional) Create a new user account. Under **Administration** > **Access Control**, select **Roles**, then create a new role with a name of your choice (for example, "Nessus").
3. Select the **VMware vSphere Lifecycle Manager** category.
4. Under **Lifecycle Manager: Image Privileges**, select **Read**.
5. (Optional) To perform compliance scans, also select **Global → Settings**.
6. Click **Create**.
7. Go to the **Inventory** page and right-click the root vCenter object at the top of the left-hand tree.
8. Click **Add Permission**.
9. Select the user account and the role you created.
10. Select **Propagate to children**, then click **OK**.
11. Run a Tenable scan to verify the permissions work.

To create a minimally privileged ESXi user role:

1. Log in to the ESXi server.
2. (Optional) Create a new user account:
    a. Under **Navigator**, expand **Host**.
    b. Select **Manage**.
    c. Select **Users**.
    d. Click **Add user**.
3. Under **Navigator**, select **Host**.
4. Click **Actions**, then select **Permissions**.

5. Select the user you want to use as a read-only user, then click **Assign role**.
6. Select **Propagate to all children**, then click **Assign role**.
7. Run a Tenable scan to verify that credentialed checks are enabled on the ESXi host.

Required User Role: Some compliance audits – specifically those with "Bare Metal" in the name – require an SSH credential, and that SSH user must be an **administrator-level** ESXi user. A read-only user cannot be used. This requirement applies only to the SSH user needed by Bare Metal audits.

Note: Because the VMware vCenter API credential supports both a SOAP and a REST connection method, and Tenable selects between them by version, the scan configuration below covers both. Configure the credential once. No version-specific credential selection is required.

Scan Configuration – VMware vCenter API

Complete the following steps to configure Tenable One Vulnerability Management with the VMware vCenter API integration.

1. Log into your Tenable One Vulnerability Management user interface.
2. In the left navigation pane, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click **Create a Scan**.

   The **Select a Scan Template** page appears.
4. Select the **Advanced Network Scan** template.

   The scan configuration page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type the IP addresses of the vCenter host and, if you are not using Auto-Discovery, the ESXi host or hosts.
7. (Optional) Add a description, folder location, scanner location, and target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.

9. Next to **Add Credentials**, click the add button, then in the **Miscellaneous** section select **VMware vCenter API**.

   The **Settings** pane for the selected credential appears.

10. Configure each option below for the selected credential.

Option	Description	Required
vCenter Host	The IP address or hostname of the vCenter instance.	Yes
vCenter Port	The TCP port that vCenter listens on for communications from Tenable. By default, Tenable uses 443.	Yes
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Yes
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. If you are using a self-signed certificate, disable this setting.	No
vCenter API Authentication Method	Choose from the available authentication methods: • Username and Password (manual entry) • PAM Integration (use a specific PAM to gather vCenter API authentication credentials from the available list)	Yes
Username	The username for the vCenter server account	Yes (if

	with admin read/write access that Tenable uses to perform checks on the target system.	**Username and Password** authentication is selected)
Password	The password for the vCenter server user.	Yes (if **Username and Password** authentication is selected)
Use Auto Discovery	Option that toggles on access to configure host and virtual machine auto-discovery.	No
Auto Discover Managed VMware ESXi Hosts	Adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	No
Auto Discover Managed VMware ESXi Virtual Machines	Adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you include in your scan.	No
Report Active and Inactive Virtual Machines	Enables collection of virtual machines for active and inactive virtual machine reports. Disabling this option reduces the overall number of requests made by the scanner.	No

11. Do one of the following:
    - To save without launching the scan, click **Save**.
    - To save and launch the scan immediately, click **Launch**.

Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Note: Listing the vCenter server as a target collects the vCenter version and its vulnerabilities, but not operating system-level details. Listing the vCenter server as a target is also required for vCenter compliance scanning.

Scan Configuration – VMware ESX SOAP API

Complete the following steps to configure Tenable One Vulnerability Management with the VMware ESX SOAP API integration.

Note: Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password.

1. Log in to your Tenable One Vulnerability Management user interface.
2. In the left navigation pane, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click **Create a Scan**.

   The **Select a Scan Template** page appears.
4. Select the **Advanced Network Scan** template.

   The scan configuration page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type the IP addresses of the ESXi host or hosts.
7. (Optional) Add a description, folder location, scanner location, and target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. Next to **Add Credentials**, click the add button, then in the **Miscellaneous** section select **VMware ESX SOAP API**.

   The **Settings** pane for the selected credential appears.

10. Configure each option below for the selected credential.

Option	Description	Required
ESX SOAP API Authentication Method	Choose from the available authentication methods: • Username and Password (manual entry) • PAM Integration (use a specific PAM to gather authentication credentials from the available list)	Yes
Username	The username associated with the local ESXi account.	Yes (if **Username and Password** authentication is selected)
Password	The password associated with the local ESXi account.	Yes (if **Username and Password** authentication is selected)
Do not verify SSL Certificate	When enabled, Tenable does not validate the SSL certificate for the ESXi server. Disable this toggle if your ESXi host uses a certificate signed by a trusted CA. Disabled by default.	No

11. Do one of the following:
    - To save without launching the scan, click **Save**.
    - To save and launch the scan immediately, click **Launch**.

Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Configure the VMware Integration with Tenable Nessus

Tenable Nessus exposes two VMware credentials in the **Miscellaneous** credential category:

- **VMware vCenter API** – for vCenter servers and the ESXi hosts and virtual machines they manage. Supports vCenter 6.x through 9.x. Uses the REST API on 7.0.3+ and the SOAP API on earlier versions.
- **VMware ESX SOAP API** – for authentication directly to targeted ESXi hosts to collect VIBs and virtual machine inventory.

Required Permissions

> **Required User Role**: Standard, Administrator, or System Administrator.

Within VMware, the minimum privileges depend on which API the scan uses:

Scan Type	API Type	Permissions Needed
vCenter credential for vulnerability scanning (7.0.3+)	REST	vCenter account with read permissions, plus VMware vSphere Lifecycle Manager: Image Privileges = Read
vCenter credential for vulnerability scanning (earlier than 7.0.3)	SOAP	vCenter admin account with read and write permissions
Standalone ESXi hosts using ESXi credentials	SOAP	User = Read Only (or administrator)
Compliance scan	SOAP	Global → Settings

To create a minimally privileged vCenter user role:

1. Log in to vCenter.
2. (Optional) Create a new user account. Under **Administration** > **Access Control**, select **Roles**, then create a new role with a name of your choice (for example, "Nessus").
3. Select the **VMware vSphere Lifecycle Manager** category.
4. Under **Lifecycle Manager: Image Privileges**, select **Read**.
5. (Optional) To perform compliance scans, also select **Global → Settings**.
6. Click **Create**.
7. Go to the **Inventory** page and right-click the root vCenter object at the top of the left-hand tree.
8. Click **Add Permission**.
9. Select the user account and the role you created.
10. Select **Propagate to children**, then click **OK**.
11. Run a Tenable scan to verify the permissions work.

To create a minimally privileged ESXi user role:

1. Log into the ESXi server.
2. (Optional) Create a new user account:
    a. Under **Navigator**, expand **Host**.
    b. Select **Manage**.
    c. Select **Users**.
    d. Click **Add user**.
3. Under **Navigator**, select **Host**.
4. Click **Actions**, then select **Permissions**.
5. Select the user you want to use as a read-only user, then click **Assign role**.
6. Select **Propagate to all children**, then click **Assign role**.
7. Run a Tenable scan to verify that credentialed checks are enabled on the ESXi host.

Required User Role: Some compliance audits – specifically those with "Bare Metal" in the name – require an SSH credential, and that SSH user must be an **administrator-level** ESXi user. A read-only user cannot be used. This requirement applies only to the SSH user needed by Bare Metal audits.

Note: Because the VMware vCenter API credential supports both a SOAP and a REST connection method, and Tenable selects between them by version, the scan configuration below covers both. Configure the credential once. No version-specific credential selection is required.

Scan Configuration – VMware vCenter API

Complete the following steps to configure Tenable Nessus with the VMware vCenter API integration.

1. Log in to your Tenable Nessus user interface.
2. In the left navigation pane, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click **Create a Scan**.

   The **Select a Scan Template** page appears.
4. Select the **Advanced Network Scan** template.

   The scan configuration page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type the IP addresses of the vCenter host and, if you are not using Auto-Discovery, the ESXi host or hosts.
7. (Optional) Add a description, folder location, scanner location, and target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. Next to **Add Credentials**, click the add button, then in the **Miscellaneous** section select **VMware vCenter API**.

   The credential options appear.
10. Configure each option below for the selected credential.

Option	Description	Required
vCenter Host	The IP address or hostname of the vCenter instance.	Yes
vCenter Port	The TCP port that vCenter listens on for communications from Tenable. By default, Tenable uses 443.	Yes
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Yes
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. If you are using a self-signed certificate, disable this setting.	No
vCenter API Authentication Method	Choose from the available authentication methods: • Username and Password (manual entry) • PAM Integration (use a specific PAM to gather vCenter API authentication credentials from the available list)	Yes
Username	The username for the vCenter server account that Tenable uses to perform checks on the target system.	Yes (if **Username and Password** authentication is selected)

Password	The password for the vCenter server user.	Yes (if **Username and Password** authentication is selected)
Use Auto Discovery	Option that toggles on access to configure host and virtual machine auto-discovery.	No
Auto Discover Managed VMware ESXi Hosts	Adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	No
Auto Discover Managed VMware ESXi Virtual Machines	Adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you include in your scan.	No
Report Active and Inactive Virtual Machines	Enables collection of virtual machines for active and inactive VM reports. Disabling this option reduces the overall number of requests made by the scanner.	No

11. Do one of the following:
    - To save without launching the scan, click **Save**.
    - To save and launch the scan immediately, click **Launch**.

Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Scan Configuration – VMware ESX SOAP API

Complete the following steps to configure Tenable Nessus with the VMware ESX SOAP API integration.

Note: Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password.

1. Log in to your Tenable Nessus user interface.
2. In the left navigation pane, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click **Create a Scan**.

   The **Select a Scan Template** page appears.
4. Select the **Advanced Network Scan** template.

   The scan configuration page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type the IP addresses of the ESXi host or hosts.
7. (Optional) Add a description, folder location, scanner location, and target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. Next to **Add Credentials**, click the add button, then in the **Miscellaneous** section select **VMware ESX SOAP API**.

   The **Settings** pane for the selected credential appears.
10. Configure each option below for the selected credential.

Option	Description	Required
ESX SOAP API Authentication Method	Choose from the available authentication methods: • Username and Password (manual entry)	Yes

	• PAM Integration (use a specific PAM to gather authentication credentials from the available list)	
Username	The username associated with the local ESXi account.	Yes (if **Username and Password** authentication is selected)
Password	The password associated with the local ESXi account.	Yes (if **Username and Password** authentication is selected)
Do not verify SSL Certificate	When enabled, Tenable does not validate the SSL certificate for the ESXi server. Disable this toggle if your ESXi host uses a certificate signed by a trusted CA. Disabled by default.	No

11. Do one of the following:
    - To save without launching the scan, click **Save**.
    - To save and launch the scan immediately, click **Launch**.

Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Configure VMware vCenter API integration with Tenable Security Center

Required User Role: Administrator, or an organizational user with appropriate permissions. For more information, see Configure VMware vCenter API integration with Tenable Security Center in the Tenable Security Center documentation.

In Tenable Security Center, VMware credentials are configured as authentication settings on a scan policy, or as reusable credentials, using the **VMware vCenter API** credential type in the **Miscellaneous** category.

Required Permissions

Within VMware, the minimum privileges depend on which API the scan uses.

Scan Type	API Type	Permissions Needed
vCenter credential for vulnerability scanning (7.0.3+)	REST	vCenter account with read permissions, plus VMware vSphere Lifecycle Manager: Image Privileges = Read
vCenter credential for vulnerability scanning (earlier than 7.0.3)	SOAP	vCenter admin account with read and write permissions
Compliance scan	SOAP	Global → Settings

To create a minimally privileged vCenter user role:

1. Log in to vCenter.
2. (Optional) Create a new user account:

a. Navigate to **Administration** > **Access Control**.

b. Select **Roles**.

c. Create a new role with a name of your choice (for example, "Nessus").

3. Select the **VMware vSphere Lifecycle Manager** category.
4. Under **Lifecycle Manager: Image Privileges**, select **Read**.
5. (Optional) To perform compliance scans, also select **Global** → **Settings**.
6. Click **Create**.
7. Go to the **Inventory** page and right-click the root vCenter object at the top of the left-hand tree.
8. Click **Add Permission**.
9. Select the user account and the role you created.
10. Select **Propagate to children**, then click **OK**.
11. Run a Tenable scan to verify the permissions work.

Required User Role: Some compliance audits – specifically those with "Bare Metal" in the name – require an SSH credential, and that SSH user must be an **administrator-level** ESXi user. A read-only user cannot be used. This requirement applies only to the SSH user needed by Bare Metal audits.

Note: Because the VMware vCenter API credential supports both a SOAP and a REST connection method, and Tenable selects between them by version, the scan configuration below covers both. Configure the credential once. No version-specific credential selection is required.

Scan Configuration – VMware vCenter API

Complete the following steps to configure Tenable Security Center with the VMware vCenter API integration.

1. Log into your **Tenable Security Center** user interface.
2. In the left navigation pane, click **Scanning**. A menu appears.
3. Click **Credentials**.

   The **Credentials** page appears.

4. Click **+Add** at the top of the screen.

   The **Add Credential** page appears.

5. In the **Miscellaneous** section, click **VMware vCenter API**.

   The **Add Credential** page for that credential type appears.

6. In the **Name** box, type a name for the credential.

7. (Optional) Add a description.

8. (Optional) Add a tag to the credential.

   For more information, see Scan Configuration – VMware vCenter API in the Tenable Security Center documentation.

9. Configure each of the following options for the selected credential.

Option	Description	Required
vCenter API Authentication Method	Choose from the available authentication methods: • Password (manual entry through username and password) • PAM Integration (use a specific PAM to gather vCenter API authentication credentials from the available list)	Yes
vCenter Host	The IP address or hostname of the vCenter instance.	Yes
vCenter Port	The TCP port that vCenter listens on for communications from Tenable. By default, Tenable uses 443.	Yes
Username	The username for the vCenter server account	Yes (if

	that Tenable uses to perform checks on the target system.	**Username and Password** authentication is selected)
Password	The password for the vCenter server user.	Yes (if **Username and Password** authentication is selected)
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Yes
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. If you are using a self-signed certificate, disable this setting.	No
Use Auto Discovery	Option that toggles on access to configure host and virtual machine auto-discovery.	No
Auto Discover Managed VMware ESXi Hosts	Adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	No
Auto Discover Managed VMware ESXi Virtual Machines	Adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you include in your scan.	No

10. Click **Submit** to save your credential.

Auto-Discovery of ESXi Hosts and Virtual Machines

The Auto-Discovery feature automatically identifies and scans the ESXi hosts a vCenter server manages, as well as the virtual machines residing on those hosts. Instead of manually entering IP addresses or hostnames in your scan target settings, Auto-Discovery queries the vCenter API to retrieve a live list of managed assets and adds them to the scan. When you enable this option, the scan automatically includes all discovered ESXi hosts and, if configured, every virtual machine hosted on those discovered hosts.

Why use Auto-Discovery instead of manual target entry?

- **Scale and convenience.** For environments with large numbers of ESXi hosts and virtual machines, Auto-Discovery reduces time spent on scan creation and preparation. Target lists remain current without manual updates.
- **Reaching unroutable hosts.** Some ESXi hosts sit behind a firewall or do not accept incoming traffic, so manual entry does not work – the scanner cannot communicate with the host. Auto-Discovery allows these ESXi hosts to "live" in the scan, which at minimum enables VIB reporting for each host and lets version-based vulnerability plugins execute. See this Auto-Discovery of ESXi Hosts and Virtual Machines for additional details of this capability.

Configuration options

Option	Description	Required
Use Auto Discovery	Toggles on access to the host and virtual machine auto-discovery options.	No
Auto Discover Managed VMware ESXi Hosts	Adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	No
Auto Discover	Adds any discovered VMware ESXi hypervisor virtual	No

Managed VMware ESXi Virtual Machines	machines to the scan targets you include in your scan.	
Report Active and Inactive Virtual Machines	Enables collection of virtual machines for active and inactive VM reports. Disabling this option reduces the overall number of requests made by the scanner.	No

Prerequisites and restrictions

Caution: Tenable recommends using scanner groups containing a single scanner when using Auto-Discovery credentials, and entering only a single initial host in the scan. If multiple scanners are used in an Auto-Discovery scan, targets retrieved from the integration may be scanned multiple times.

Note: This feature is only available when scanning vCenter/ESXi versions 7.0.3 and later.

Note: Auto-Discovery does not automatically add the ability to authenticate remotely to ESXi hosts and virtual machines. You can add additional SSH credentials to authenticate to the ESXi host discovered and added to the scan, as well as SSH or Windows credentials to authenticate to virtual machines discovered and added to the scan.

Note: Compliance scanning is unavailable when Auto-Discovery is enabled. Run compliance scans with Auto-Discovery disabled and explicit vCenter/ESXi targets.

Compliance

Tenable One Vulnerability Management, Tenable Security Center, or Tenable Nessus can scan VMware environments for compliance. Compliance checks are targeted, credentialed checks of ESXi and/or vCenter servers based on the targets listed in the scan settings.

- When scanning a **vCenter** host, Tenable reports on the vCenter server and on any ESXi servers that vCenter manages.
- When scanning an **ESXi** host, the scan reports on that ESXi host.
- You can scan both ESXi and vCenter hosts in a single scan.
- The vCenter server must be listed as a scan target for vCenter compliance checks to run.

Required plugin: VMware vCenter/vSphere Compliance Checks (64455) must be enabled to execute compliance scanning. This plugin is automatically enabled when you add an audit file that requires it.

Required permissions: compliance scanning requires the **Global → Settings** privilege in vCenter, in addition to the read privileges needed for vulnerability scanning.

API behavior: compliance checks use the SOAP API regardless of vCenter version, unlike normal vulnerability checks, which use the REST API on VMware 7.0.3 and newer. This is because the SOAP API exposes configuration data at the level of detail compliance auditing requires.

Constraints:

- Compliance scanning is unavailable with the Auto-Discovery feature enabled.
- Some compliance audits – those with "Bare Metal" in the name – require an additional SSH credential configured with an administrator-level ESXi user. Adding these audits displays a notice that SSH credentials are required.
- Audit/compliance is supported on vCenter 6.x, 7.x, 8.x, and 9.x.

Scan Results Review

This section helps you interpret the results of your VMware vCenter API and VMware ESX SOAP API scans.

Plugin families and plugins

The following Tenable plugins are relevant when reviewing scan results with the VMware integration.

Misc. plugin family:

- **Plugin #204872: Integration Status.** When using a Tenable integration with any PAM Integration, the Integration Status plugin confirms whether credential retrieval succeeded or failed.

General plugin family:

- **Plugin #168417: Integration Discovered Host** – reports targets that were added to the scan by an integration's auto-discovery feature. vCenter is a Tenable integration that supports auto-discovery of ESXi hosts and virtual machine hosts.

Settings plugin family:

- **Plugin #19506: Nessus Scan Information** – see the following Caution. This plugin's Credentialed Checks value reflects VIB collection, not host login.

> **Caution**: Tenable has observed user confusion about **Credentialed Checks: yes/no** in plugin 19506 and how authentication is interpreted for the VMware integrations. In a traditional SSH or Windows scan, that value reflects whether login credentials to the target machine were valid. With the VMware integrations, Tenable authenticates to the vCenter or ESXi *API* – not the host machine. Unless an SSH credential is included alongside the VMware credential, expect **Credentialed Checks: yes** if the integration collected VIBs for that host and **no** if it did not. When scanning vCenter-managed ESXi hosts with API credentials, the vCenter host's own results always show **Credentialed Checks: No**.

Service Detection plugin family:

- **Plugin #63061: VMware vCenter Detect** – gathers the vCenter version from an unauthenticated SOAP API call to the vCenter host. Even later versions (7.0.3+) maintain a SOAP API. The version this plugin gathers feeds vCenter vulnerability detection plugins that rely on versioning, and determines whether the integration collects vCenter and ESXi data via the SOAP API (earlier than 7.0.3) or the REST API (7.0.3+). This plugin runs independently of the integration and **is not indicative of vCenter authentication issues**.
- **Plugin #57396: VMware vSphere Detect** – gathers the ESXi version from an unauthenticated SOAP API call to the ESXi host. The version feeds ESXi vulnerability detection plugins that rely on versioning. This plugin runs independently of the integration and **is not indicative of authentication issues**.

VMware ESX Local Security Checks plugin family:

- **Plugin #63062: VMware vCenter Data Collection** – handles authentication to the vCenter REST API and collection of vCenter-managed ESXi hosts, ESXi VIBs, ESXi-managed virtual machines, and virtual machine details, for vCenter and ESXi 7.0.3+. Collection and storage execute against only one target in the scan and are reused for reporting on subsequent enumerated targets.
- **Plugin #180178: VMware vCenter Legacy Data Collection** – the equivalent plugin for the vCenter SOAP API, used for vCenter and ESXi versions earlier than 7.0.3.
- **Plugin #180179: VMware vCenter Auto-Discovery** – executes the auto-discovery process when Auto-Discovery of ESXi hosts and virtual machines is enabled.
- **Plugin #154017: VMware vCenter Managed ESXi Installed VIBs** – reports the installed VIBs collected on a vCenter-managed ESXi host. Credentialed Checks status and version-based detections depend on successful VIB collection. Tenable does not run vulnerability detections against the specific VIB data itself.
- **Plugin #57400: VMware vSphere Installed VIBs** – reports the installed VIBs collected directly on an ESXi host through the ESX SOAP API.
- **Plugin #84340: VMware vCenter Active Virtual Machines** – reports powered-on virtual machines collected for a specific ESXi host, reported against that ESXi host.

- **Plugin #84341: VMware vCenter Inactive Virtual Machines** – reports powered-off virtual machines collected for a specific ESXi host.
- **Plugin #57397: VMware Active Virtual Machines** – the ESX SOAP API equivalent for powered-on virtual machines.
- **Plugin #57398: VMware Inactive Virtual Machines** – the ESX SOAP API equivalent for powered-off virtual machines.

> **Note**: In addition to these integration-related plugins, ESXi vulnerability detection plugins belong to the VMware ESX Local Security Checks plugin family. If this plugin family is disabled, scan results do not include those vulnerability detections.

Policy Compliance plugin family:

- **Plugin #64455: VMware vCenter/vSphere Compliance Checks** – must be enabled to execute compliance scanning and performs compliance checks against both vCenter and ESXi hosts.

Debug Log Reporting

Debugging log report output is controlled by the debug logging settings in Tenable Nessus. Review the debugging log files related to the specific credential being used, when troubleshooting scans with the VMware vCenter API or VMware ESX SOAP API integration.

> **Note**: Plugin debugging for VMware is **not** centralized in a single log. The vCenter path writes to a per-collection-host debug log, while the ESXi SOAP path writes separate logs per feature (VIBs, active VMs, inactive VMs). ESXi SOAP API authentication occurs in each of those, so check all of them when troubleshooting a standalone ESXi scan.

vCenter authentication and data collection

Path	Debug log
vCenter REST API (7.0.3+)	vmware_vcenter_collect.nbin~Collection_host
vCenter SOAP API (earlier than 7.0.3)	vmware_vcenter_collect_legacy.nbin~Collection_host

The Collection_host is the IP address or FQDN of the host the collection was executed on, which happens only once per scan. These logs contain all aspects of data collection: authentication, retrieval of all ESXi hosts managed by the vCenter, VIBs installed for each ESXi host, virtual machines hosted on each ESXi host, and virtual machine details.

ESXi SOAP API logs

Data collected	Debug log
ESXi installed VIBs	vmware_installed_vibs.log
ESXi active virtual machines	vmware_active_vms.log
ESXi inactive virtual	vmware_inactive_vms.log

machines	
Compliance checks	vmware_compliance_check.log, vmware_compliance_check_debug.log

Caution: Do not use the debug logs for **VMware vCenter Detect (63061)** or **VMware vSphere Detect (57396)** – including **vmware_vsphere_detect.log** – to diagnose authentication problems. These plugins always send unauthenticated calls, so their logs can be misleading and do not represent authentication success or failure.

What the logs contain

The debug logs record the full integration lifecycle for each scan, including:

- Configuration settings loaded from the scan policy (with sensitive values masked).
- The authentication method used and whether authentication succeeded.
- The VMware vCenter API requests and the HTTP response status.
- Details on host(s), virtual machine, and VIBs collection.
- Any errors returned by the VMware vCenter API, including authentication failures.

Common causes of Credentialed Checks: no on an ESXi host

- Authentication to the vCenter API failed, so no data was retrieved.
- The host was not returned as a managed ESXi host for the vCenter server in the credential, so VIBs were not retrieved for it.
- The host is managed by vCenter, but the request to collect VIBs for that specific host returned an error – commonly a permissions problem on VMware vSphere Lifecycle Manager.
- Verify SSL Certificate is enabled in the scan policy while the vCenter server presents a self-signed certificate.
- The environment is a mixed-version deployment in which the REST API is unavailable on some hosts.

Additional Information

Helpful Tips

At a high level, the integration performs the following sequence on each scan:

1. Detects vCenter and ESXi versions with unauthenticated calls, which determines whether collection uses the SOAP or REST API.
2. Authenticates to the vCenter API (bearer/session token) or to the ESXi SOAP API using the configured credential.
3. Enumerates the ESXi hosts the vCenter server manages.
4. Collects installed software components (VIBs) for each managed ESXi host and stores them in the scanner's Knowledge Base.
5. Enumerates virtual machines per ESXi host and retrieves virtual machine details, reporting active and inactive virtual machines against the applicable host.
6. If Auto-Discovery is enabled, adds discovered ESXi hosts and virtual machines to the scan as additional targets.
7. If compliance audits are configured, collects configuration data over the SOAP API and evaluates the audit checks.

Practical guidance:

- Collection runs once per scan against a single target and is reused for the remaining targets — so a failure at the collection step affects reporting for every enumerated host.
- Always list the vCenter server as a target when you want vCenter vulnerability results or vCenter compliance results.
- Run the curl tests below **from the scanner** so that network connectivity to the vCenter host is exercised at the same time as permissions.
- Disable **Report Active and Inactive Virtual Machines** in very large environments where virtual machine inventory is not needed, to reduce scan duration and request volume.

Testing Integration Connectivity

The following curl commands mirror the integration's own REST API request flow (vCenter 7.0.3+). The following curl commands also contain environmental variables (for example, `${VCENTER_USERNAME}`). If you are not familiar with using variables, you can use manual entry within the commands. Options are provided for both in each section.

vCenter API authentication

Tenable uses bearer token authentication authorized to the vCenter username/password entered in the scan credentials. You can use this simple curl command test to ensure that this user has the appropriate permissions and to rule out any authentication issues to the vCenter REST API before running a scan.

You can choose to export environmental variables, such as `VCENTER_USERNAME`. The following curl commands are formatted for environmental variables. You can also manually enter these values. If executed manually, an example of the username:password of the authentication command may look like this:

```
-u 'myuser:mypassword'
```

```
curl -k -X POST -u "${VCENTER_USERNAME}:${VCENTER_PASSWORD}" https://${VCENTER}/api/session
```

Manual entry option:

- Replace "`${VCENTER_USERNAME}:${VCENTER_PASSWORD}`" with -u 'myuser:mypassword'.
- Replace `${VCENTER}` with your vCenter IP address or FQDN.

A successful response yields a session token that can be used for subsequent requests. Example of a successful response, which is the session token to be used in subsequent requests: "`7b08862e67aa48f758c627fc2aa710a6`".

If you do not obtain a session token, the following table lists some possible reasons why.

Reason	Status code	Server response
Incorrect username and/or password	401 Unauthorized	error_type: `UNAUTHENTICATED`, `"Authentication required."`
Incorrect vCenter host, host does not support the REST API, or SSL certificate verification was enabled in the scan policy	500 Server Error	`Error 500 Server Error`, or no response at all

List the ESXi hosts vCenter manages

If authentication to the vCenter REST API was successful, Tenable then makes a request to vCenter to gather a list of ESXi hosts that it manages. This list of ESXi hosts is enumerated in subsequent requests.

To test this, run the following curl command:

```
curl -k -X GET -H "vmware-api-session-id: ${SESSION}" https://${VCENTER}/api/vcenter/host
```

Manual entry option:

- Replace `${SESSION}` with the value received from the authentication request.
- Replace `${VCENTER}` with your vCenter IP address or FQDN.

If successful, expect the following response: `Status Code 200: OK`

Server Response:

```
[
  {
    "host": "host-1006",
```

```
    "name": "1.1.1.1",
    "connection_state": "CONNECTED",
    "power_state": "POWERED_ON"
  },
  {
    "host": "host-1007",
    "name": "1.1.1.2",
    "connection_state": "CONNECTED",
    "power_state": "POWERED_ON"
  },
  {
    "host": "host-1008",
    "name": "1.1.1.3",
    "connection_state": "CONNECTED",
    "power_state": "POWERED_ON"
  }
]
```


List installed software components (VIBs) per ESXi host

In this request, Tenable asks vCenter to report on the installed software components (VIBs) for each of the ESXi hosts it manages. Take the "host" (host-id) for any of the list of hosts from the previous call to test the following command, which rules out any permission errors:

```
curl -k -X GET -H "vmware-api-session-id: ${SESSION}" https://${VCENTER}/api/esx/hosts/${ESX_
HOST}/software/installed-components
```

The `${ESX_HOST}` value should be one of the "host" values received from the request to get a list of ESXi hosts managed by the vCenter.

Manual entry option:

- Replace `${SESSION}` with the value received from the authentication request.
- Replace `${VCENTER}` with your vCenter IP address or FQDN.
- Replace `${ESX_HOST}` with one of the "host" values received from the request to get a list of ESXi hosts managed by the vCenter.

A successful response yields similar results: `Status Code 200: OK`

Server Response:

```
{
  "Broadcom-ELX-IMA-plugin": {
    "display_version": "12.0.1200.0-6vmw",
    "display_name": "Broadcom IMA plugin for Emulex OneConnect iSCSI Driver",
    "version": "12.0.1200.0-6vmw.800.1.0.20513097",
    "platforms": ["host"]
  },
  "Broadcom-ELX-brcmfcoe": {
    "display_version": "12.0.1500.3-4vmw",
    "display_name": "Broadcom Emulex Connectivity Division fcoe driver for FCoE adapters",
    "version": "12.0.1500.3-4vmw.800.1.0.20513097",
    "platforms": ["host"]
  },
  "Broadcom-ELX-lpfc": {
    "display_version": "14.0.635.4-14vmw",
    "display_name": "Broadcom Emulex Connectivity Division lpfc driver for FC adapters",
    "version": "14.0.635.4-14vmw.800.1.20.21203435",
    "platforms": ["host"]
  },
  "esx-update": {
    "display_version": "8.0.0 Build 21493926",
    "display_name": "ESXi Install/Upgrade Component",
    "version": "8.0.0-1.25.21493926",
    "platforms": ["host"]
  },
  "esxio-update": {
    "display_version": "8.0.0 Build 21493926",
    "display_name": "ESXi Install/Upgrade Component",
    "version": "8.0.0-1.25.21493926",
    "platforms": ["host"]
  }
}
```


Most often, if you do not have the correct vCenter Lifecycle Manager permissions, you receive the following response (refer to the permissions section for proper configuration): `Status Code 403: UNAUTHORIZED`

Server Response:


```
{
  "error_type": "NOT_FOUND",
  "messages": [
```

```
    {
      "args": [],
      "default_message": "Not found.",
      "id": "com.vmware.vapi.rest.httpNotFound."
    }
  ]
}
```

List virtual machines on one ESXi host

Tenable sends a request to the vCenter API to get a list of virtual machines hosted on a specific ESXi host. This list of virtual machines is enumerated in subsequent requests.

```
curl -f -k -X GET -H "vmware-api-session-id: ${SESSION}" https://${VCENTER}/api/vcenter/vm?hosts=${ESX_
HOST}
```

Manual entry option:

- Replace `${SESSION}` with the value received from the authentication request.
- Replace `${VCENTER}` with your vCenter IP address or FQDN.
- Replace `${ESX_HOST}` with one of the "host" values received from the request to get a list of ESXi hosts managed by the vCenter.

Retrieve details for a specific virtual machine

From the list of virtual machines, you can take one of the virtual machine IDs (for example, `vm-1024`) and send a request to vCenter to retrieve virtual machine details for that specific virtual machine. The `${VM}` value should be one of the "vm" values received from the request to get a list of virtual machines hosted on the ESXi server.

```
curl -f -k -X GET -H "vmware-api-session-id: ${SESSION}"
https://${VCENTER}/api/vcenter/vm/${VM}/guest/identity
```

Manual entry option:

- Replace `${SESSION}` with the value received from the authentication request.
- Replace `${VCENTER}` with your vCenter IP address or FQDN.
- Replace `${VM}` with one of the "vm" values received from the request to get a list of virtual machines hosted on the ESXi server.

If a virtual machine is powered off, this results in a status code of `503 Service Unavailable`. If this happens, run the following alternative command.

```
curl -f -k -X GET -H "vmware-api-session-id: ${SESSION}" https://${VCENTER}/api/vcenter/vm/${VM}
```

Manual entry option:

- Replace `${SESSION}` with the value received from the authentication request.
- Replace `${VCENTER}` with your vCenter IP address or FQDN.
- Replace `${VM}` with one of the "vm" values received from the request to get a list of virtual machines hosted on the ESXi server.

Frequently Asked Questions

Why do my vCenter scan results show Credentialed Checks: "No" even though authentication succeeded?

That is expected. When scanning vCenter-managed ESXi hosts with API credentials, the vCenter host's results always show **Credentialed Checks: No**. Check the ESXi hosts' results instead — **Credentialed Checks: Yes** there means that VIBs were collected successfully. Plugin 204872 (Integration Status) is the most direct way to confirm integration authentication.

An ESXi host shows Credentialed Checks: No. Where do I start?

Check the vCenter collection debug log (vmware_vcenter_collect.nbin~Collection_host for 7.0.3+), then run the curl tests in **Testing integration connectivity** from the scanner. The most common causes are failed vCenter authentication, the host not being returned as a managed ESXi host, or missing vSphere Lifecycle Manager read privileges.

Why can't I run a compliance scan and Auto-Discovery in the same scan?

Compliance scanning is unavailable when Auto-Discovery is enabled. Use two scans: one with Auto-Discovery for vulnerability coverage, and another scan (SSH or SMB) with explicit vCenter/ESXi targets for compliance.

My environment has vCenter 7.0.3 managing older ESXi hosts. Is that supported?

No. Mixed-version environments where the REST API is unavailable on some hosts are not supported. vCenter 8 managing ESXi 7.0.3 is supported.

Does the integration report on the guest operating systems of my virtual machines?

No. The VMware credentials collect management-tier data only. Add SSH or Windows credentials targeting the guest operating systems to assess them.

Why does my Auto-Discovery scan appear to scan the same host more than once?

Auto-Discovery scans should use a scanner group containing a single scanner, with a single initial host entered in the scan. With multiple scanners, targets retrieved from the integration can be scanned multiple times.