

# VMware Skyline Health Diagnostics Installation, Configuration, and Operations Guide

VMware Skyline Health Diagnostics

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

## About VMware Skyline Health Diagnostics 6

## 1 Installing VMware Skyline Health Diagnostics 7

Overview of Installing VMware Skyline Health Diagnostics 7

Installation Requirements 8

Downloading the Software Images 8

Download VMware Skyline Health Diagnostics Virtual Appliance OVA 9

Download VMware Skyline Health Diagnostics ISO Install Media File for Offline Deployment and Updates - Deprecated 9

Downloading update packages for Offline Update 9

Password Policy 10

Deploying VMware Skyline Health Diagnostics 10

Deploy VMware Skyline Health Diagnostics Using the OVA Image 11

Migrate the existing VMware Skyline Health Diagnostics Instance to Version 3.0 or Later 13

How to get the VMware Skyline Health Diagnostics Appliance out of Suspended Mode 15

## 2 Configuring VMware Skyline Health Diagnostics 17

Managing Software Updates 17

View Download and Update History 17

Check, Download and Install Software Updates 18

Update using Offline Patch Bundle 19

Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful 20

Check and Download VMware Compatibility Guide (VCG) Updates 21

Managing the Behavior and Performance 22

Update the Value of the Configuration Property 24

Manage the VMware Skyline Health Diagnostics Services 24

Configuring Notification Feature of VMware Skyline Health Diagnostics 25

Configure SMTP Server Settings for Email Notifications 25

Configure the Notification Distribution Group 28

Managing Proxy Settings 30

Enable Proxy Settings 30

Deactivate Proxy Settings 31

Configuration for Proxies acting as MITM (Man-In-The-Middle) 32

Managing User Accounts 33

Add User Accounts 33

Update User Accounts or Reset Password 37

Delete User Account 43

Participating in the Customer Experience Improvement Program	44
Manage Customer Experience Improvement Program Status	44
Managing SSL Certificates	45
Custom Certificate Requirements	45
Generate Certificate Signing Request	45
Replace the Self-Signed Certificate with the Custom Certificate	46
Reverting to Self-Signed Certificate	47
<b>3 Using the VMware Skyline Health Diagnostics</b>	<b>49</b>
Log in to VMware Skyline Health Diagnostics from Web Browsers	49
Operations in the VMware Skyline Health Diagnostics	50
Direct Connect and Analyze (Live or Online Analysis)	51
Working with Analysis Profiles and Schedules	51
Scheduling Analysis Runs	62
Supported Diagnostic Checks for Products and Related Input Requirements as part of Analysis Profile	64
Offline Log Bundle Based Analysis	67
Summary of Supported Products, Analysis Mode, and Checks Available	69
Interacting with the VMware Skyline Health Diagnostics using REST API	70
Authenticating with the VMware Skyline Health Diagnostics REST API Server	70
Using the API Explorer	71
Summary of available REST APIs	71
Working with Analysis Reports	73
View Analysis Reports in VMware Skyline Health Diagnostics	73
Delete Analysis Report in the VMware Skyline Health Diagnostics	75
Save or Delete Multiple Analysis Reports	75
Configuring Auto Delete for Analysis Reports	76
Interpret the Diagnostics Report of the VMware Skyline Health Diagnostics	77
Interpret VCG or vSAN HCL Validation Summary	82
Interpret VMware Cloud Foundation Health Checks Report	83
Interpret VMware vSAN Storage Report	84
Interpret the VMware Horizon Report	85
Interpret the VMware SD-WAN Products report	86
Add and Remove Tags for the Analysis Report	87
Search and view the Analysis Reports	87
Registering VMware Skyline Health Diagnostics Plug-in with VMware vCenter Server	88
Registration of Plug-in from vSphere Client 80 U1 and onwards	88
Registration of Plug-in from VMware Skyline Health Diagnostics User Interface	91
Using the Plug-in from vSphere Client	92
Refresh registered VMware vCenter Server	93
Deregistration of Plug-in from VMware Skyline Health Diagnostics User Interface	94
Help and Support	95

[View the CEIP Data Collected for Reporting and Analytics](#) 96

## **4** [Scale Limits for VMware Skyline Health Diagnostics](#) 98

[Scale Limits](#) 98

## **5** [Ports and Protocols](#) 100

## **6** [Supported Versions and Compatibilities](#) 102

# About VMware Skyline Health Diagnostics

The VMware Skyline Health Diagnostics is a self-service health and diagnostics platform that can help users detect and troubleshoot issues in their VMware environment. The platform uses log bundles, configuration & health information, and other data to identify potential problems, and suggest relevant VMware Knowledge Base articles or remediation steps which can be helpful in resolving complex issues for the vSphere, vSAN, VMware Cloud Foundation, VMware Horizon, and VMware SD-WAN products. It can work in internet connected and offline mode. Users can use this solution to monitor the health of the environment, performing security, pre-upgrade, drivers, and hardware health checks, and troubleshooting issues in the environment before contacting to the VMware Support. This guide provides information on installing, configuring, and operating the VMware Skyline Health Diagnostics.

## Intended Audience

System administrators who want to install and configure the VMware Skyline Health Diagnostics. This information is written for experienced system administrators who are familiar with VMware vSphere virtual machine management and data center operations.

# Installing VMware Skyline Health Diagnostics

# 1

Your environment must fulfill certain requirements so that you can install VMware Skyline Health Diagnostics.

Read the following topics next:

- [Overview of Installing VMware Skyline Health Diagnostics](#)
- [Installation Requirements](#)
- [Downloading the Software Images](#)
- [Password Policy](#)
- [Deploying VMware Skyline Health Diagnostics](#)

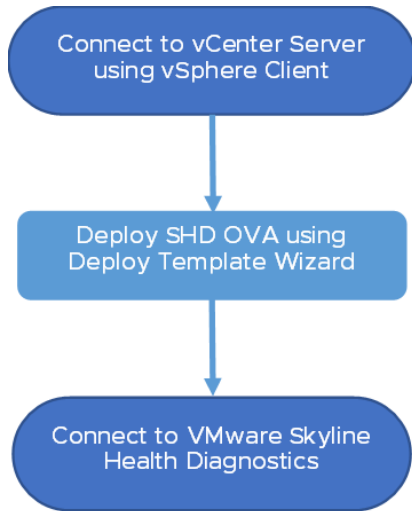
## Overview of Installing VMware Skyline Health Diagnostics

Installing VMware Skyline Health Diagnostics involves deploying an appliance using an OVA. During the deployment, you need to provide the IP address or FQDN, network settings, passwords for the VMware Photon operating system `root` and `shd-admin` user. `shd-admin` is the VMware Skyline Health Diagnostics administrator and web interface user.

Before installing the VMware Skyline Health Diagnostics, you must download the VMware Skyline Health Diagnostics appliance OVA from the [VMware Customer Connect site](#).

The naming pattern for the appliance image OVA is `VMware-Skyline-HealthDiagnostics-Appliance-<product_version>-<build_number>_OVF10.ova` where `product_version` and `build_number` are the current available version and build number of the VMware Skyline Health Diagnostics.

The appliance is pre-configured with required software and settings to run the VMware Skyline Health Diagnostics. The VMware Skyline Health Diagnostics can be deployed in a single step through the vSphere Web Client connected to the VMware vCenter Server.

**Figure 1-1. Installation Steps for VMware Skyline Health Diagnostics.**

## Installation Requirements

The environment must fulfill certain requirements so that you can install the VMware Skyline Health Diagnostics.

### Software Requirement

- VMware vCenter Server 6.5 or later.
- VMware ESXi Host 6.5 or later.

### Compute and Storage Requirements

The VMware Skyline Health Diagnostics appliance virtual machine requires,

Number of vCPUs	4
Memory	16 GB
Storage - Thin Provisioned	2 GB
Storage - Thick Provisioned (Preferred)	250 GB

### Ports and Protocols

The VMware Skyline Health Diagnostics requires network connectivity to the vSphere products for running the analysis. Ensure [ports and protocols requirements](#) are met.

## Downloading the Software Images

You can download the VMware Skyline Health Diagnostics OVA from VMware Skyline Health Diagnostics product download page before installation.



## Download VMware Skyline Health Diagnostics Virtual Appliance OVA

Installing the VMware Skyline Health Diagnostics using virtual appliance image OVA is very simple and fast process.

### Prerequisites

- Verify that your system has a web browser and can connect to the internet.
- Verify that you have credentials to log in to My VMware account at [VMware Customer Connect](#) site, and you can access [VMware Skyline Health Diagnostics product download](#) page.

### Procedure

- 1 Go to [VMware Skyline Health Diagnostics product download](#) page using the web browser from your system.
- 2 Click on **Download Now** of OVA image file for VMware Skyline Health Diagnostics, the naming pattern for the appliance image OVA is `VMware-Skyline-HealthDiagnostics-Appliance-<product_version>-<build_number>_OVF10.ova`.
- 3 Read the **End User License Agreement** in the popup window and click accept to start the OVA download.

### Results

The VMware virtual appliance file for VMware Skyline Health Diagnostics is downloaded.

## Download VMware Skyline Health Diagnostics ISO Install Media File for Offline Deployment and Updates - Deprecated

Download and install of the VMware Skyline Health Diagnostics using the ISO install media file has been deprecated starting from version 4.0 onwards.

---

**Attention** Follow the [Migrate the existing VMware Skyline Health Diagnostics Instance to Version 3.0 or Later](#) to upgrade ISO based installs to the VMware Skyline Health Diagnostics version 4.0.0.

Post migrated to Version 4.0.0, you can use the Offline Path Bundle for future update/patching of the VMware Skyline Health Diagnostics (Refer: [Downloading update packages for Offline Update](#))

---

## Downloading update packages for Offline Update

Download and install of the VMware Skyline Health Diagnostics using the ISO install media file has been deprecated starting from version 4.0 onwards. Updating offline instances (VMware Skyline Health Diagnostics deployments without internet connectivity) requires an offline patch or update bundle.

## Prerequisites

- Verify that your system has a web browser and can connect to the internet.
- Verify that you have credentials to log in to My VMware account at [VMware Customer Connect](#) site, and you can access [VMware Skyline Health Diagnostics product download](#) page.

## Procedure

- 1 Go to [VMware Skyline Health Diagnostics product download](#) page using the web browser from your system.
- 2 Click on **Download Now** of Offline Patch file for VMware Skyline Health Diagnostics, the naming pattern for the Offline Patch Bundle is `VMware-shd-patch-offline-product_version>-<build_number>.tar.gz`.
- 3 Read the **End User License Agreement** in the popup window and click accept to start with Offline Patch Bundle download.

## Results

The Offline Patch bundle for VMware Skyline Health Diagnostics is downloaded.

# Password Policy

You must follow the security and compliance guidelines for the password established by your organization, or the VMware recommended globally accepted standard guideline to ensure the safety and security of the infrastructure.

The password must contain at least eight characters, have characters from at least two classes from Group One (lowercase and uppercase characters and numbers) and at least one character from the class Group Two (Special Characters).

- Valid Character Class Group One: `[a-z], [A-Z], [0-9]`
- Valid Character Class Group Two: `[~!@#$$%^&]`

For example,

- `Th1lsISV@l1d`
- `ThisIsVali$Too`
- `ThisisnotValld`

# Deploying VMware Skyline Health Diagnostics

Deploy the VMware Skyline Health Diagnostics Appliance to VMware ESXi host managed by the VMware vCenter Server.

The VMware Skyline Health Diagnostics OVA deployment is simplified and is a one-step process. Connect to the VMware vCenter Client and deploy the downloaded OVA Image. After the successful deployment, the VMware Skyline Health Diagnostics appliance is ready for use.

---

**Note** VMware Skyline Health Diagnostics by default creates a user *shd-admin* with Administrator Role at the time of initial configuration. This user account must not be deleted and the only account available post deployment. You can use this account to login and create further user accounts.

---

## Deploy VMware Skyline Health Diagnostics Using the OVA Image

You can deploy the VMware Skyline Health Diagnostics using a pre-configured OVA image.

### Prerequisites

- Download the OVA image for the VMware Skyline Health Diagnostics from [VMware Skyline Health Diagnostics product download](#).
- Verify that you can access vSphere Infrastructure with privileges required for creating and interacting with virtual machines.
- Verify that you have host, storage, and network configuration details for the virtual appliance being deployed, refer to the Installation Requirements section for the appliance deployment requirements.

### Procedure

- 1 In the vSphere Client connected to the VMware vCenter Server, right-click the datacenter or cluster or host on which you want to deploy the VMware Skyline Health Diagnostics virtual appliance.
- 2 Click **Deploy OVF Template** to start the deployment process.
- 3 Perform the followings steps:
  - a On the **Select an OVF template** page, select Local file, and click **Upload files**.
  - b On the Open dialog page, select the OVA file, click **Open**, and click **Next**.
- 4 On the **Select a name and folder** page, in the **Virtual machine name** text box, enter the name for the VMware Skyline Health Diagnostics virtual appliance. Select the preferred datacenter, or cluster, or host for the virtual machine and click **Next**.
- 5 On the **Select a compute resource** page, select the preferred VMware ESXi host as the compute resource, and click **Next**.
- 6 On the **Review details** page, review the settings, and click **Next**.
- 7 On the **License agreements** page, accept the license agreement, and click **Next**.
- 8 On the **Select storage** page, select the destination storage and optionally the preferred format and the storage policy, and click **Next**.

- 9 On the **Select networks** page, select the port group to which you want the appliance to connect and click **Next**.
- 10 On the **Customize template** page, configure following settings, and click **Next**.

a

Settings	Value
Initial/Current root password	The password of the <i>root</i> user of VMware Photon operating system as per the security compliance policy of your organization or <a href="#">Password Policy</a> . The password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.
Initial/Current <i>shd-admin</i> user password	The password for the <i>shd-admin</i> user account as per the security compliance policy of your organization or <a href="#">Password Policy</a> . The password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.  <b>Note</b> VMware Skyline Health Diagnostics by default creates a user <i>shd-admin</i> with Administrator Role. This user account must not be deleted and the only account available post deployment. You can use this account to login and create further user accounts.
Host Name	Enter the hostname or FQDN for the appliance (leave blank in case DHCP is desired).
Network IP Address	Enter the IP address for the appliance (leave blank in case DHCP is desired).
Network Prefix	Enter the network prefix for the appliance (leave blank in case DHCP is desired).
Default IPv4 Gateway	Enter the default gateway for the appliance (leave blank in case DHCP is desired).
Domain Name Servers	Enter the IP address of the primary and secondary DNS servers, comma or space separated values are accepted (leave blank in case DHCP is desired).
NTP Servers	Enter the NTP server or servers. Enter comma or space separated values if entering multiple NTP servers. NTP servers can be entered using FQDNs or IP addresses.

- 11 On the **Ready to complete** page, click **Finish**, and wait for the completion of the task.

Power on newly deployed virtual machine. The OS boots up and the appliance is ready to use in approximately five minutes.

## Results

The VMware Skyline Health Diagnostics virtual appliance is deployed and configured.

## Migrate the existing VMware Skyline Health Diagnostics Instance to Version 3.0 or Later

You can migrate any 2.x.x version of the VMware Skyline Health Diagnostics instance to 3.0 and later using the migration method. This will ensure your previous configurations and analysis reports are preserved and migrated to the new instance.

### Prerequisites

- If you are using the VMware Skyline Health Diagnostics version earlier than 2.5.0, first upgrade to version 2.5.x, and then migrate to version 3.0 or later.
- A direct migration from 2.0.x version to 3.0.x or later version is not possible.
- IP address of the source VMware Skyline Health Diagnostics appliance and it must be reachable from the IP address and FQDN of the new appliance.
- Download the OVA image for the VMware Skyline Health Diagnostics from [VMware Skyline Health Diagnostics product download](#).
- Verify that you can access vSphere Infrastructure with privileges required for creating and interacting with virtual machines.
- Verify that you have host, storage, and network configuration details for the virtual appliance being deployed, refer to the [Installation Requirements](#) section for the appliance deployment requirements.

### Procedure

- 1 In the vSphere Client connected to the VMware vCenter Server, right-click the datacenter or cluster or host to which you want to deploy the VMware Skyline Health Diagnostics virtual appliance.
- 2 Click **Deploy OVF Template** to start the deployment process.
- 3 Perform the followings steps:
  - a On the Select an OVF Template page, select **Local File**, and click **Upload Files**.
  - b On the Open dialog page, navigate to the OVA file, click **Open**, select file, and click **Next**.
- 4 On the **Select a name and folder** page, in the **Virtual machine name** text box, enter the name for Skyline Health Diagnostics virtual appliance. Select a destination folder for the virtual machine and click **Next**.
- 5 On the **Select a compute resource** page, select the VMware ESXi host for the compute resource, and click **Next**.
- 6 On the **Review details** page, review the settings, and click **Next**.
- 7 On the **License agreements** page, accept the license agreement, and click **Next**.
- 8 On the **Select storage** page, select the destination storage and optionally the format and storage policy, and click **Next**.

9 Select the port group to which you want the appliance to connect and click **Next**.

10 On the **Customize Template** page enter the details and click **Next**.

a Enter the values of the settings.

Settings	Value
Initial/Current root password	<p>The password of the <i>root</i> user of VMware Photon operating system as per the security compliance policy of your organization or <a href="#">Password Policy</a>.</p> <p>The password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.</p>
Initial/Current <i>shd-admin</i> user password	<p>The password for the <i>shd-admin</i> user account as per the security compliance policy of your organization or <a href="#">Password Policy</a>.</p> <p>The password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.</p> <hr/> <p><b>Note</b> VMware Skyline Health Diagnostics by default creates a user <i>shd-admin</i> with Administrator Role. This user account must not be deleted and the only account available post deployment. You can use this account to login and create further user accounts.</p>
Existing VMware-SHD instance IP or Hostname	The Network IP or FQDN of an existing SHD instance, use for migrating the old deployment to new instance (Do not leave this field empty).
Existing VMware-SHD instance IP or Hostname	The Network IP or FQDN of an existing SHD instance, use for migrating the old deployment to new instance (Do not leave this field empty).
Host Name	Enter the hostname or FQDN for the appliance (leave blank in case DHCP is desired).
Network IP Address	Enter the IP address for the appliance (leave blank in case DHCP is desired).
Network Prefix	Enter the network prefix for the appliance (leave blank in case DHCP is desired).
Default IPv4 Gateway	Enter the default gateway for the appliance (leave blank in case DHCP is desired).
Domain Name Servers	Enter the IP address of the primary and secondary DNS servers, comma or space separated values are accepted (leave blank in case DHCP is desired).
Search Domains	DNS Search Domains [comma (,) or space-separated]. (Leave blank if DHCP is desired)
NTP Servers	Enter the NTP server or servers. Enter comma or space separated values if entering multiple NTP servers. NTP servers can be entered using FQDNs or IP addresses.

- 11 On the **Ready to complete** page, click **Finish**, and wait for the completion of the process.
- 12 After the deployment complete, power on newly deployed virtual machine.

The Appliance boots up and finishes the initial configuration in approximately five minutes. Time required to complete the initial configuration may vary depending upon the amount of data on the source VMware Skyline Health Diagnostics instance.

## Results

The VMware Skyline Health Diagnostics virtual appliance is deployed, and the configuration and report data are migrated to this new instance.

## What to do next

- After verifying that all the configurations and reports on newly migrated instance are intact, decommission the older instance of the VMware Skyline Health Diagnostics virtual appliance.
- The IP address of the newly deployed instance is different from the previous one. In case, you want to reuse the older IP address. After you decommission the older VMware Skyline Health Diagnostics instance, you can assign the same IP to a new instance.

## How to get the VMware Skyline Health Diagnostics Appliance out of Suspended Mode

If the initial configuration is suspended due to weak password. The VMware Skyline Health Diagnostics - First Boot Password Manager page will be displayed and you will not be able to move beyond this page.

The VMware Skyline Health Diagnostics appliance requires strong passwords for both `root` and `shd-admin` user account. If the passwords do not meet the [Password Policy](#) requirements, the initial configuration is suspended until you complete the configuration by entering a strong password using the VMware Skyline Health Diagnostics user interface. You can configure password for the VMware Skyline Health Diagnostics appliance as described in this section.

## Prerequisites

Verify that your system has a web browser installed and can connect to the internet.

## Procedure

- 1 Connect to the VMware Skyline Health Diagnostics appliance using a web browser **`https://FQDN_OR_IP_ADDRESS_OF_VMwareSkylineHealthDiagnostics`**.

If you don't see a page with title **VMware Skyline Health Diagnostics for vSphere - First Boot Password Manager**, you don't need to perform any further configuration and your appliance is ready for use.

- 2 Enter the details as requested.

You need to provide the passwords entered at deploy time and new password. For the password, follow the security compliance policy of your organization or [Password Policy](#)

- 3 Click `Submit` to complete the configuration.
- 4 After completing the appliance configuration, the appliance will reboot after one minute.

## Results

Initial password configuration for the appliance is complete.

## What to do next

- After appliance is rebooted, open a Web browser and go to `https://FQDN_OR_IP_ADDRESS_OF_VMwareSkylineHealthDiagnostics` to access the user interface, the login page will be displayed.
- Log in using the credentials for `shd-admin` account.
- User accounts can be added using **User Management** section under **Settings** in the user interface.



# Configuring VMware Skyline Health Diagnostics

## 2

You can perform administrative tasks on the VMware Skyline Health Diagnostics application.

Read the following topics next:

- [Managing Software Updates](#)
- [Managing the Behavior and Performance](#)
- [Configuring Notification Feature of VMware Skyline Health Diagnostics](#)
- [Managing Proxy Settings](#)
- [Managing User Accounts](#)
- [Participating in the Customer Experience Improvement Program](#)
- [Managing SSL Certificates](#)

## Managing Software Updates

You must keep the VMware Skyline Health Diagnostics appliance up to date with the latest releases to get the latest features, bug fixes, improved diagnostics capabilities, and recommendation on the issues.

## View Download and Update History

You can view past downloads and upgrade history of the VMware Skyline Health Diagnostics.

### Prerequisites

- Verify that you can open the VMware Skyline Health Diagnostic user interface in a web browser.
- Verify that you have the valid credentials to log in to the VMware Skyline Health Diagnostic.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Upgrade & History**.

- 4 Click the **Tool Update** tab, to see the **Upgrade History Summary** and **Download History Summary** sections.
- 5 Click **VCG Update** tab, to see the VMware Compatibility Guide related upgrade and downloads.

### Results

The **Upgrade History Summary** section displays the last five upgrade activities.

The **Download History Summary** section displays the last five download activities.

### What to do next

You can optionally check and download new updates by clicking on **Check Tool Updates** button the under **Tool Update** tab.

## Check, Download and Install Software Updates

You can get benefited from the latest signatures released for the VMware Skyline Health Diagnostics by frequently checking for updates, downloading, and applying the updates.

Check and download new updates for the VMware Skyline Health Diagnostics.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that VMware Skyline Health Diagnostics has internet connectivity to the VMware sites listed in the [Outbound Interaction](#) section.
- If you plan to download the updates, verify that you are logged in with the administrator privileged user credentials.

---

**Caution** Take the snapshot of the VMware Skyline Health Diagnostics appliance virtual machine before installing the new updates.

---

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Upgrade & History**.
- 4 Click the **Tool Update** tab.
- 5 To check if the new updates are available, click **Check Tool Updates**.  
If new updates are available, a download option is displayed for the user with administrator privileged.
- 6 To download the update, click **Download Updates**.
- 7 Confirm that the version is visible in **Download History Summary**.

- 8 After the updates are downloaded, reboot the VMware Skyline Health Diagnostics appliance by, opening the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client. Log in as a `root` user and run the command `reboot`. On startup, the software is updated automatically.

### Results

New updates are downloaded.

### What to do next

- 1 Verify that the operation is successful using the steps mentioned in [Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful](#).

## Update using Offline Patch Bundle

You can get benefited from the latest signatures released for the VMware Skyline Health Diagnostics by frequently checking for updates, downloading, and applying the updates. For appliances without internet connectivity you can use the Offline Patch Bundle to complete the update process.

Perform offline update of the VMware Skyline Health Diagnostics.

### Prerequisites

- Make sure you have already downloaded the Offline Patch Bundle for the **VMware Skyline Health Diagnostics**, follow the [Downloading update packages for Offline Update](#).
- Verify that you have an SSH client like Putty installed and can access.
- VMware Skyline Health Diagnostics Appliance over SSH (Port 22).
- Verify that you have valid `root` user credentials for VMware Skyline Health Diagnostics Appliance.
- Verify that you have valid `shd-admin` user credentials for VMware Skyline Health Diagnostics.
- Verify that you have remote file copy utilities like WinSCP installed on the system where you have the Offline Patch Bundle downloaded.

---

**Caution** Take the snapshot of the VMware Skyline Health Diagnostics appliance virtual machine before installing the new updates.

---

### Procedure

- 1 Copy the downloaded Offline Patch Bundle file to folder `/opt/vmware-shd/vmware-shd/temp` on the VMware Skyline Health Diagnostics appliance using remote file copy client like WinSCP.
- 2 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 3 Log in as **root** user.

- 4 Change directory to the folder to which you have copied the Offline Patch Bundle `cd /opt/vmware-shd/vmware-shd/temp`.

- 5 Extract the Offline Patch Bundle using tar utility `tar -zxvf VMware-shd-patch-offline-product_version-<build_number>.tar.gz`.

The Offline Patch Bundle extracted to a folder with naming pattern `vmware-shd-patch-<product-version>`.

- 6 Run the patch staging utility `stageupdate` found within the extracted patch folder `vmware-shd-patch-<product-version>/stageupdate`.

- 7 When prompted, please enter the password for user `shd-admin`.

The Offline Patch Bundle will be validated and staged for updating the instance.

- 8 Confirm the restart of Skyline Health Diagnostics appliance by pressing any key.

Appliance will be restarted. On startup, the software is updated automatically.

---

**Note** Press `Ctrl+C` to roll back the staging.

---

## Results

The appliance upgraded to the desired version using the Offline Patch Bundle.

## What to do next

- 1 Verify that the operation is successful using the steps mentioned in [Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful](#).

## Verify the Update or Upgrade of VMware Skyline Health Diagnostics is Successful

You can verify the VMware Skyline Health Diagnostics update or upgrade is successful with few simple checks.

### Prerequisites

- Verify that you can open the user interface of the VMware Skyline Health Diagnostics in the browser window.
- Verify that you are logged in with the administrator privileged user credentials.
- Verify that the VMware Skyline Health Diagnostics is connected to internet.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **About**.

- 4 Take the note of version information. It should display the version you downloaded to upgrade to.
- 5 In the left pane, select **Upgrade & History**.
- 6 Select the **Tool Update** tab and refer to **Download History Summary & Upgrade History Summary**. You can ensure these sections are displaying latest version you downloaded. If the version information is consistent, it means that the update or upgrade is successful.
- 7 If **Upgrade History Summary** or **About** section information is not updated with latest downloaded or intended version, it means that the update or upgrade operation has failed. Please collect the log bundle and send email to **shd-support@vmware.com**.
- 8 If the update or upgrade is successful, delete the snapshot of the virtual machine.
- 9 If the update or upgrade fails, revert to the snapshot taken before the upgrade and then delete the snapshot.

### Results

You have successfully verified the update or upgrade of VMware Skyline Health Diagnostics.

## Check and Download VMware Compatibility Guide (VCG) Updates

You can get benefited from the latest VMware compatibility guide updates released for the VMware ESXi hosts, hardware, and IO devices by frequently checking for **VCG Updates** and downloading the updates.

Check and download new updates for VCG Database using [VMware Compatibility Guide](#)

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that the VMware Skyline Health Diagnostics have internet connectivity to <https://shd-download.vmware.com>. Refer to the [Outbound Interaction](#) section for checking the ports and protocols used for interacting with the site.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Upgrade & History**.
- 4 Click the **VCG Update** tab.

## 5 Click the **Update VCG Database** to download the VCG updates.

VCG and vSAN HCL data is refreshed with the latest data from the VMware Compatibility Guides.

### Results

**Note** Note: The update can take about approximately from 30 through 40 minutes to complete. Once started, the process runs asynchronously and post update, VMware Compatability Guide Database details are updated in the user interface. You can proceed with other activities in the user interface without blocking the updates.

VMware Compatability Guides database is updated on the VMware Skyline Health Diagnostics appliance.

## Managing the Behavior and Performance

You might want to change various settings for the VMware Skyline Health Diagnostics appliance for better user experience and performance. The configuration settings are now available in the user interface.

Only **shd-admin** user or users with the administrative privilege can modify the properties from the VMware Skyline Health Diagnostics user interface.

Configuration Properties	Description
Log File Size	This property indicates the maximum allowed file size for Skyline Health Diagnostics logs. If the size of the logs exceeds this value, the logs are overwritten. Note the value is specified in Megabyte (MB).
Log File Count	This property indicates the number of Skyline Health Diagnostics log files that will be retained after log rotation.
Password History	This property indicates the number of saved passwords that were used previously. <b>Note:</b> You cannot reuse any of the saved passwords.
Password expiry (in days)	This property indicates the duration (in days) for which a password can be used. Beyond this period, the UI authentication will fail. You can set the value as 90 or 180 days.
Log in Failure Count	This property specifies the permitted number of authentication failures before the user account is locked. Setting to <b>0</b> will deactivate Account Lockout.
Log in Failure Window	This property specifies the duration in minutes to track authentication failures before account lockout.
Account Lockout Duration	This property specifies the duration in minutes the account remains locked. During this time, the user is disallowed from logging in to VMware Skyline Health Diagnostics.

Configuration Properties	Description
Log Analyze Limit	The duration in days for which log events are analyzed from the log collection time. Setting the value to <b>0</b> will deactivate.
Number of Log Indexers	This property specifies the number of log indexers deployed for log indexing. The log indexer helps to index the logs. Faster indexing results in faster log analysis and report generation. The recommended number of indexers value is $n-1$ , where $n$ is the number of vCPUs of the VMware Skyline Health Diagnostics virtual machine. As the default number of vCPUs for the appliance are four so, you keep the value to three.
Number of Log Extractors	This property specifies the number of log extractions that can run in parallel.
Log Generation Timeout	This property is used during the log collection phase of the analysis operation, it specifies duration in minutes for which analysis waits for log bundle generation to complete. The value being <b>0</b> indicates no timeout.
Log Download Timeout	This property is used during the log collection phase of the analysis operation, it specifies duration in minutes for which the analysis workflow waits for log bundle download to complete. The value being <b>0</b> indicates no timeout.
Log Extraction Timeout	This property used during the log extraction phase of analysis operation; it specifies duration in minutes for which the analysis workflow will wait for log bundle extraction to complete. The value being <b>0</b> indicates no timeout.
SSH Keep alive Timeout	This property specifies duration in minutes for which a workflow will wait for an SSH connection to respond.
Show Owned Reports Only	This property allows access to the reports that are generated as part of analysis initiated by you. You will not be able to see the reports from other users. Note: <b>shd-admin</b> has access to all the reports.
Report Retention Period	The period in days after which a report is deleted automatically. Use <b>0</b> to deactivate auto delete.
HTTP or HTTPS Connection Timeout	This property specifies the duration in seconds to wait before the external HTTP or HTTPS connection timeout.
Scheduler run frequency	How often the scheduler checks for the pending schedules (in seconds)
Max Schedule Submit Task	Max parallel schedules can be submitted
Notification Backlog Processing Frequency	How often the notification backlog is processed (in seconds)
Notifications Retry Count	How many times Email Notification will be retried on transient failures



## Update the Value of the Configuration Property

You can update the value in the configuration property to change the behavior and performance of the appliance.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Configuration**.
- 4 Select the property you want to modify.
- 5 Click the edit button  to update the property value.
- 6 Enter a value for the property and Click **Ok**.
- 7 Click  OK button to save the value.

### Results

The value of the property is updated.

## Manage the VMware Skyline Health Diagnostics Services

You can configure the services for VMware Skyline Health Diagnostics running on the appliance.

A web server and an application server together are responsible for providing UI and diagnostics capabilities of the VMware Skyline Health Diagnostics. The server is implemented in the form of services whose settings are auto configured. You need not change the settings unless the technical support guides you.

---

**Note** All the services are configured to auto start on the system startup.

Server Component	Service Name	Description
Web server	Nginx	It provides web user interface through the browser.
Application Server	vmware-shd	Handles upload and diagnostics for log bundles.



### Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.

### Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Run command `systemctl` to start, stop, restart, and check status `systemctl start|status|restart|stop SERVICE_NAME`.

### Results

The service is started, restarted, or stopped as per the input parameters.

## Configuring Notification Feature of VMware Skyline Health Diagnostics

You can enable the notification feature to receive the report of the analysis over an email.

### Configure SMTP Server Settings for Email Notifications

You can configure SMTP setting to receive notifications for the analysis completion or failure along with the analysis report over the email.

### Add SMTP Server Settings

You can add **SMTP Server Settings** to receive notifications for the analysis completion or failure along with the analysis report over the email.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

- Verify that you have SMTP server, port, user name, password, and email address of the sender.

**Caution** The VMware Skyline Health Diagnostics does not support SMTP server behind the proxy. You must use local SMTP server or internal SMTP server in such case.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Notification Settings**.
- 4 On the **Email** tab, enter the SMTP configuration details and click **Add**.

Property	Value
Server	Enter the SMTP server FQDN or IP address.
Port	Enter the SMTP server port.
User name	Enter the user name.
Password	Enter the password.
Security	Set the security to None or STARTTLS or SSL-Implicit as appropriate.
Sender	Enter the sender's email address.

#### Results

The configuration for email notification is encrypted and saved.

**Example: Settings for Microsoft Office 365 and Local Host SMTP server.**

**Settings for Microsoft Office 365 as SMTP server.**

Refer to Microsoft Office documentation and check with your respective administrator to configure the Office 365 SMTP server. Following is an example for using Office 365 SMTP server.

Property	Value
Server	smtp.office365.com
Port	587
User name	user@domain.com
Password	Password for user@domain.com
Security	TLS-STARTTLS
Sender	user@domain.com

## Settings the Local host as SMTP server.

You can use `local host` with port 25 leaving the user name and password empty. Set the security as `None`. Following is an example for using `local host` SMTP server.

Property	Value
Server	Local host
Port	25
User name	Optional
Password	Optional
Security	None
Sender	shd-support@test.com

### What to do next

Add Distribution Group configuring the email address of recipients.

## Delete SMTP Server Settings

You can delete **SMTP Server Settings** to stop receiving the notifications from the VMware Skyline Health Diagnostics.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you have configured the **SMTP Server Settings** on the VMware Skyline Health Diagnostics.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Notification Settings**.
- 4 On the **Email** tab, click **Delete**.

The SMTP Server Setting removed are removed from the VMware Skyline Health Diagnostics.

## Configure Notification Batch Frequency and Retry Behavior

Pending Notifications are sent in a batch mode at configured interval instead of at the end of analysis run. In default, configuration notifications backlog is processed every one minute. There

is a retry mechanism to retry failed notifications. By default, retry count is set to three. You can change both these settings based on your requirements.

### Prerequisites


- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you have SMTP server, port, user name, password, and email address of the sender.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Configuration**.

To modify how often notification backlog is processed, modify the **Notification Backlog Processing Frequency** parameter.

To modify how often the notifications retry will be performed, modify the **Notification Retry Count** parameter.

- 4 Click the **Edit**  icon, enter the value and close the dialog box, new value should be saved.

### Results

The configuration for notification processing and retry is updated.

## Configure the Notification Distribution Group

You can configure the **Notification Distribution Group** of add email addresses of members for receiving the analysis reports from the VMware Skyline Health Diagnostics.

### Create Notification Distribution Group

You can send the report of an analysis run to one or more VMware vSphere or VMware Cloud Foundation administrators, operators, or delegates. You can achieve this by adding one or more member's email addresses to distribution group and receive the report of analysis run.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

- Verify that you have configured the **SMTP Server settings**.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Notification Settings**.
- 4 On **Email** tab, in **Notification Distribution Group** pane, click Add and enter the details.

Property	Value
Name	Enter the distribution group name.
Emails	Enter a comma separated list of emails address of respective administrator or users email Id to create group.

#### Results

The notification distribution group is created.

## Modify the Notification Distribution Group

You can modify the notification distribution group to add email addresses of new member or remove from the existing list.

#### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you have configured the Email **SMTP Server settings**.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click **Settings** tab from the top-menu.
- 3 In the left pane, select **Notification Settings**.
- 4 On **Email** tab in **Notification Distribution Group** pane, select the distribution list that you want to modify.
- 5 Click **Edit** button.
- 6 Add or Remove email addresses.
- 7 Click **Save**.

## Results

The notification distribution group is modified.

## Delete the Notification Distribution Group

You can delete the notification distribution group if it is not required anymore.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you have configured the Email **SMTP Server settings**.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click **Settings** tab from the top-menu.
- 3 In the left pane, select **Notification Settings**.
- 4 On **Email** tab in **Notification Distribution Group** pane, select the distribution group that you want to delete.
- 5 Click **Delete** icon, click **Delete** button from the confirmation pop up.

## Results

The notification distribution group is deleted.

## Managing Proxy Settings

You can configure the proxy settings on the VMware Skyline Health Diagnostics appliance to use the proxy server for any inbound or outbound connection from the appliance.

## Enable Proxy Settings

You can enable the proxy settings on the VMware Skyline Health Diagnostics appliance by using the user interface.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you have the details of proxy server and user credentials (if any).

- If your proxy is configured to act as MITM, see section [Configuration for Proxies acting as MITM \(Man-In-The-Middle\)](#) before configuring the proxy.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click **Settings** tab from the top-menu.
- 3 In the left pane, select **Proxy Settings**.
- 4 Click the **Edit** in the top-right corner of the proxy pane.

Edit option available only when proxy is deactivated.

The **Edit Proxy Settings** dialog box appears.

- 5 Enter the required details related to proxy.

Property	Value
URL	Enter the FQDN/IP of proxy server (only HTTPS is supported protocol).
Port	Enter the port number of the proxy server.
User Name	Enter the user name for authenticating into the proxy server.  This is optional and only required if authentication is enabled on the proxy server.
Password	Enter the password for authenticating into the proxy server.  This is optional and only required if authentication is enabled on the proxy server.
Anonymous	Use this option anonymous authentication is configured on the proxy server.

- 6 If no user credentials are required for proxy access, select the **Anonymous** checkbox.
- 7 To check whether the entered details are correct, click **Check connection**.
- 8 Once the **Check connection** operations completes successfully click **Submit**.

#### Results

Proxy server information is updated the VMware Skyline Health Diagnostics appliance.

## Deactivate Proxy Settings

You can deactivate the proxy settings on the VMware Skyline Health Diagnostics appliance by using the user interface.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that **Proxy Settings** are enabled on the VMware Skyline Health Diagnostics.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Proxy Settings**.
- 4 Deactivate the proxy if it is enabled by toggling the **Enabled** button.

### Results

Proxy server is deactivated on the VMware Skyline Health Diagnostics appliance.

## Configuration for Proxies acting as MITM (Man-In-The-Middle)

Your organization might have proxy servers acting as a firewall and web filter, providing shared network connections, and cache data to speed up common requests. Such proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet. You will require configuration on the appliance running the VMware Skyline Health Diagnostics to work with such proxies. Without this configuration, HTTPS connections from the VMware Skyline Health Diagnostic will fail to verify the proxy generated certificates and result in failures.

### Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.
- Make sure you have the `root` certificate, or the certificate used by proxy to sign the certificates used for connections. Normally this will be root certificate of your internal CA.

### Procedure

- 1 Open the Root or Proxy Certificate in a text editor and copy the contents.



- 2 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 3 Log in as **root** user.
- 4 Create a temporary file to save the copied certificate,
  - a Run the command `vi /tmp/proxy.crt`
  - b Press **I** to change to insert mode.
  - c Paste the copied contents.
  - d Press **Esc** to switch the insert mode off.
  - e Press **:wq** to save and quit the editor.
- 5 To update the VMware Skyline Health Diagnostics installation with newly created proxy certificate run the command `shd-config proxycert/tmp/proxy.crt`.
- 6 To Configure the proxy, see [Enable Proxy Settings](#) section.

## Results

Proxy Certificates are installed on the VMware Skyline Health Diagnostics appliance.

# Managing User Accounts

You can manage users using the VMware Skyline Health Diagnostics user interface or from the console, using commands.

---

**Caution** The VMware Skyline Health Diagnostics has one built-in administrative account `shd-admin` which cannot be removed, only users with Administrator Role can perform administrative tasks.

---

## Add User Accounts

As an Administrator, you can add another users accounts into the VMware Skyline Health Diagnostics.

### Adding an Administrator Account

As an Administrator, you can add another administrator accounts into the VMware Skyline Health Diagnostics.

An administrator account can be added to the VMware Skyline Health Diagnostics using the user interface.

#### Add an Administrator Account by using the User Interface

As an Administrator, you can add another administrator accounts in the VMware Skyline Health Diagnostics who has privileges to perform diagnostics, health, security, driver status scans on

the environment. In addition to it, administrator can perform user management, update the configuration settings, and perform updates on the VMware Skyline Health Diagnostics.

### Prerequisites

- Verify that you can connect to the VMware Skyline Health Diagnostics appliance user interface in browser.
- Verify that you have administrator privileged user credentials for the VMware Skyline Health Diagnostics.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 From the top menu, select **Settings** tab.
- 3 In the left pane, select **User Management**.
- 4 In **Local User** tab, click **Add User** to add new user.
- 5 In the **Create Local User** dialog box, provide the details.

Property	Value
Name	Enter the Full name of the user.
Email Id	Enter the email id of the user.
User Name	Enter the desired user name used for log into the user interface.
Password	Enter the password.
Confirm Password	Confirm the password.
Choose User Role	Select the <b>Choose User Role</b> value as <b>SHD Administrator</b> .

- 6 Click **Submit**.

### Results

A new administrator account is created.

## Adding an Operator Account

As an Administrator, you can add operator accounts into the VMware Skyline Health Diagnostics who has privileges to perform diagnostics, health, security, driver status scans on the environment or you can delegate the task of troubleshooting the log bundle to other operators with restricted privileges.

An operator account can be added to the VMware Skyline Health Diagnostics by:

- Using the VMware Skyline Health Diagnostics user interface.

- Appliance console.

### Add an Operator Account by using the User Interface

You can create an operator account using the VMware Skyline Health Diagnostics user interface.

#### Prerequisites

- Verify that you can connect to the VMware Skyline Health Diagnostics appliance user interface in browser.
- Verify that you have administrator privileged user credentials for the VMware Skyline Health Diagnostics.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 From the top menu, select **Settings** tab .
- 3 In the left pane, select **User Management**.
- 4 In **Local User** tab, click **Add User** to add new user.
- 5 In the **Create Local User** dialog box, provide the details.

Property	Value
Name	Enter the Full name of the user.
Email Id	Enter the email id of the user.
User Name	Enter the desired user name used for log into the user interface.
Password	Enter the password.
Confirm Password	Confirm the password.
Choose User Role	Select the <b>Choose User Role</b> value as <b>SHD Operator</b> .

- 6 Click **Submit**.

#### Results

A new operator account is created.

### Add an Operator Account by using the Appliance Console

You can create an operator account using commands on the VMware Skyline Health Diagnostics appliance console.

#### Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.

- Verify that you have password for `shd-admin` user.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.

#### Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Invoke `User Management` by running the `shd-user` command.
- 4 Enter the password for the user `shd-admin`.

If the `shd-admin` password was not set during the deployment, you must now set it now.

- 5 To add user, select the option 2. `Add new user account`.
- 6 Set a username and password for this new account.

For the password, follow the security compliance policy of your organization or [Password Policy](#)

#### Results

A new operator account is created.

## Add VMware vCenter Server Users to VMware Skyline Health Diagnostics

You can add existing VMware vCenter Server users in the VMware Skyline Health Diagnostics.

#### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you have log in credentials for the VMware vCenter Server.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 From the top menu, click on the **Settings** tab .
- 3 In the left pane, select **User Management** and click **External User** tab.

- 4 Click the **Add user** to add external user from the VMware vCenter Server.
- 5 Enter the values for the properties and click **Submit**.

Property Name	Value
User Name	Enter the user name assigned to the user to be added.
Email Id	Enter the email address of the user to be added.
Full Name	Enter the full name of the user to be added.
Provider	Enter the VMware vCenter Server FQDN or IP address.

- 6 Click **Submit**.

### Results

VMware vCenter Server user is added to the VMware Skyline Health Diagnostics.

## Update User Accounts or Reset Password

You can update user account details according to the organizational security compliance policy or reset a password expiring.

You can reset or change the user details from the VMware Skyline Health Diagnostics user interface or from the command line interface.

### Reset User Password Before Expiry using the User Interface

A user can change its password before expiry from the VMware Skyline Health Diagnostics user interface.

#### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click **Settings** tab from the top-menu.
- 3 In the left pane, select **Reset Password**.

- 4 You can reset the password for the current logged in user in the `Reset Password for user` wizard.

Property	Value
Current Password	Enter the current password for the logged in user.
New Password	Enter the new password.
Confirm Password	Confirm the new password.

- 5 Click **Submit**.

## Results

The password has been successfully updated for the logged in user.

## Update User Details or User Password using the User Interface

You can change the user details from the VMware Skyline Health Diagnostics user interface.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
  - Verify that you have credentials for user with *SHD Administrator* role for the VMware Skyline Health Diagnostics instance on which you plan to modify a user details.
- 
- **Note** You can use this option for resetting the expired password for any other existing account, by logging into the VMware Skyline Health Diagnostics with a working **SHD Administrator** user account.
- 

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click **Settings** tab from the top-menu.
- 3 In the left pane, select **User Management**.
- 4 Select the user name for which you want to update the details or reset the password.
- 5 Select the user from the list and click **Edit** button.
- 6 In the **Edit User** dialog box .

Property	Value
Name	Enter the updated value of Full name.
Change Password	Select this option for updating the password of the selected user.
New Password	Enter the new password.

Property	Value
Confirm Password	Confirm the new password.
Choose User Role	Select the <b>Choose User Role</b> value as <b>SHD Operator</b> .

7 Edit the user details and click **Update**.

## Results

The user details and password are updated.

## Update or Reset User Password using the Console

You can reset or change the user password using the VMware Skyline Health Diagnostics command line interface.

### Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- Verify that you have password for `shd-admin` user.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.

### Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 To start user management run the command `shd-user`.
- 4 When prompted, enter the password for `shd-admin`.  
Set the password for `shd-admin` now if you did not set it during the installation.
- 5 To change the password, select **Change password for a user** option from the menu.
- 6 To reset the password, select **Reset password for a user** option from the menu.
- 7 When prompted, enter the user name for which the action to be performed.  
If prompted, enter the `shd-admin` password again.

- 8 Enter the new password for the user and confirm it.

For the password, follow the security compliance policy of your organization or [Password Policy](#)

## Results

The password is successfully reset or updated for the user.

## Resetting the Expired Password for `shd-admin`

If the `shd-admin` password has expired, you cannot use the user interface to reset it, and you must reset it using the `root` credentials on the virtual machine console instead. The VMware Skyline Health Diagnostics version 4.0.0 and above supports an option of `force` resetting the password for `shd-admin` account in case user do not remember the current password.

## Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- Verify that you have password for `shd-admin` user.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.
- You can only reset the expired password if you have the current expired password for the `shd-admin` user.

## Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Run the command **`shd-config resetadmin`**.
- 4 Provide the expired password when prompted.

If the password is not correct you will have an option to force reset. Type **YES** to force reset in case you do not remember the last used password.

- 5 Enter the new password and confirm it.

For the password, follow the security compliance policy of your organization or [Password Policy](#)



## Results

The `shd-admin` user password is updated.

## Configuring Password Rotation and Account Lockout Policies

You can configure password rotation and account policies for the VMware Skyline Health Diagnostics.

You can customize password and account lockout policies based on your organization policies. These settings are stored in the configuration file `/opt/vmware-shd/vmware-shd/app/apiserver/vmware-shd.conf` in the `[account]` section.

Element	Description	Parameter	Default	Minimum	Maximum
Password History	Number of previous passwords to be stored. You cannot repeat these passwords till the limit exhausted. Setting the value to 0 the password changes history is not tracked.	<code>account/history</code>	3	0	5
Maximum password age	The maximum age of a password in days after which UI authentication will fail with password expired error.	<code>account/passage</code>	90	1	No Limit
Log in Failure window	The amount of time in minutes within which successive log in failures count towards locking an account.	<code>account/failwindow</code>	5	1	No Limit

Element	Description	Parameter	Default	Minimum	Maximum
Log in Failure Count	The number of successive failures tolerated before locking the account.	account/ failcount	0	1	No Limit
Account Lockout duration	The duration in minutes account stays locked.	account/ locktime	15	1	No Limit

**Caution** You must restart the VMware Skyline Health Diagnostics service by running the `systemctl restart vmware-shd` command for the new changes to be effective.

### Change Password and User Account Policies

An administrator might need to change the default password and account policies by changing the default password expiration period of ninety days.

#### Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.

#### Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Navigate to folder by running the command `cd /opt/vmware-shd/vmware-shd/app/apiserver/`.
- 4 Backup the current configuration file by running the command `cp vmware-shd.conf vmware-shd.conf.back`.
- 5 Edit the configuration file using `vim` editor by running the command `vim vmware-shd.conf`.
- 6 In `vi` editor, press the **Insert** key to switch to the edit mode.
- 7 Change the value for the required field.
- 8 To save and exit the editor, press **Esc** key and type `:wq`.

- Restart the services by running the `systemctl restart vmware-shd` command.

## Updating the User Details Imported from VMware vCenter Server

You may want to update the details for a user imported from the VMware vCenter Server.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

### Procedure

- Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- Click **Settings** tab from the top-menu.
- In the left pane, select **User Management** and then select **External User** tab.
- Select the user you want to update the details.
- Click the **Edit User** button to update the user from the VMware vCenter Server.
- Update the **User Name** or, **Recipient Email Id** and click **Update**.

### Results

The VMware vCenter Server user details are updated.

## Delete User Account

As an Administrator, you can delete users, except the default `shd-admin` user account from the VMware Skyline Health Diagnostics.

### Delete User Account by using the User Interface

You can delete a user account using the VMware Skyline Health Diagnostics user interface.

### Prerequisites

- Verify that you can connect to the VMware Skyline Health Diagnostics appliance user interface in browser.
- Verify that you have administrator privileged user credentials for the VMware Skyline Health Diagnostics.

---

**Caution** You cannot delete the default `shd-admin` user account from the VMware Skyline Health Diagnostics.

---

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 From the top menu, select **Settings** tab .
- 3 In the left pane, select **User Management**.
- 4 In **Local User** tab, select the user you want to delete.
- 5 Click **Delete User** to remove user.
- 6 Click **Delete** from the pop up.

### Results

A new user account is deleted.

## Participating in the Customer Experience Improvement Program

When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of the VMware products and services.

This product participates in the VMware Customer Experience Improvement Program (CEIP). For more information about CEIP and the purposes for which it is used by VMware, go to the Trust and Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

## Manage Customer Experience Improvement Program Status

It is optional to join the Customer Experience Improvement Program (CEIP). You can join or leave the program at any time.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click **Settings** tab from the top-menu.
- 3 In the left pane, select **Customer Experience Improvement Program**.
- 4 In the **CEIP Status** section, select or change your CEIP preference.
  - a If already joined the program and want to opt out, click **Joined** and click **Leave** in the resulting Leave CEIP confirmation dialog box.
  - b If you haven't joined yet and want to join the CEIP, click **Not Joined**.
- 5 Click **Show Data** to view the sample of data that is being collected under the CEIP program.

## Managing SSL Certificates

You can configure SSL certificates for the VMware Skyline Health Diagnostics appliance.

The VMware Skyline Health Diagnostics uses SSL certificates to encrypt communications between the server and the client browser to securely access and process the data. By default, the server uses self-signed certificates generated during the installation. You may want to use the trusted certificates. You can obtain a custom certificate that meets your organization's guidelines and update the VMware Skyline Health Diagnostics appliance to use those certificates. Ensure custom certificate meets [Custom Certificate Requirements](#).

### Custom Certificate Requirements

The custom certificate must satisfy several requirements to adhere to the security standards.

Ensure the certificate meets your organization's compliance and security policy.

Element	Requirement
Key size	2048 bits (minimum) to 16384 bits (maximum)
Key Encoding	PEM
Key Format	CRT
SSL Version	x509 version 3
SubjectAltName	It must have the FQDN value of the VMware Skyline Health Diagnostics appliance.

### Generate Certificate Signing Request

You can replace the default certificates with custom certificates as per the organization policy and practice to enforce the standard compliance and security practices. To replace a certificate, generate a certificate signing request as per the guidance from your organization or by using the steps described in this section. You may want to get the certificate signed by certificate authority and replace the certificates for the VMware Skyline Health Diagnostics appliance.

#### Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.

## Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as **root** user.
- 3 To navigate to the root directory, run the command `cd /`.
- 4 Create a directory under the root folder on the VMware Skyline Health Diagnostics appliance, run the command `mkdir newcert`.
- 5 Change the working directory to the new directory, run the command `cd newcert`.
- 6 Copy the configuration file to the present location, run the command `cp /opt/vmware-shd/vmware-shd/conf/ssl/conf ./..`.
- 7 Edit the configuration as required,
  - a Edit the configuration file using `vi` editor, by using `vi conf`.
  - b Match your organization details, edit the `[req_distinguished_name]` section.
  - c Set the entries for `commonName` and `DNS.1` to match the FQDN of the appliance.
- 8 Generate a new certificate signing request, run the command `openssl req -new -config conf -newkey rsa:2048 -nodes -keyout rui.key -out rui.csr`.  
Key and certificate signing request (CSR) files are created in the current directory. (`rui.csr`, `rui.key`).
- 9 Use the `rui.csr` file for signing request from the certificate authority.

## Results

The certificate signing request is generated.

## What to do next

Send the certificate signing request file `rui.csr` to your certificate authority for signing.

## Replace the Self-Signed Certificate with the Custom Certificate

You can replace the default self-signed certificate with a custom certificate signed by your certificate authority to meet the organizations security compliance guidelines.

## Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).

- Verify that you can log in using **root** credentials to the VMware Skyline Health Diagnostics appliance console.
- Verify that you have the signed SSL Certificate with the Certificate Signing Request generated in [Generate Certificate Signing Request](#) section.

#### Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as **root** user.
- 3 Change the working directory to the directory you created while generating the Certificate Signing Request, run the `cd your_directory_name` command. For example, `cd newcert`.
- 4 Create a new file by name `rui.crt` using `vi` editor, run the command `vi rui.crt`.
- 5 Copy the contents of CA signature that you received from your CA authority, open the CA signed certificate on your desktop using any text editor and copy the content.
- 6 Paste the content to the `rui.crt` file using `vi` editor, press **I** to enable insert mode.  
You must see - **INSERT** - in the bottom of the screen pressing the insert mode.
- 7 Right-click to paste the copied certificate details.
  - a If your CA provides any intermediate certificates, make sure you copy and paste them following the actual certificate.
- 8 Save the file by pressing the following sequence `Esc:wq`.
- 9 Copy the previously generated key and certificate files to the location where default certificate is located.
  - a `cp rui.crt rui.key /opt/vmware-shd/vmware-shd/conf/ssl/`
- 10 Restart the web server, run the command `systemctl restart nginx`.
- 11 Log in to the user interface using browser and verify that the new certificate is used.

#### Results

The web server runs with custom certificates.

#### What to do next

If the VMware Skyline Health Diagnostics user interface is not available, revert to self-signed certificate see [Reverting to Self-Signed Certificate](#).

## Reverting to Self-Signed Certificate

If the attempt to replace the self-signed certificates with custom certificates fails, an administrator must revert to the self-signed certificate.

## Prerequisites

- Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.

## Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Run the command `shd-config refreshcert`.

## Results

The VMware Skyline Health Diagnostic appliance services starts using the refreshed self-signed certificate.



# Using the VMware Skyline Health Diagnostics

## 3

This guide provides information to perform various operations in the VMware Skyline Health Diagnostics user interface in web browser.

Read the following topics next:

- [Log in to VMware Skyline Health Diagnostics from Web Browsers](#)
- [Operations in the VMware Skyline Health Diagnostics](#)
- [Direct Connect and Analyze \(Live or Online Analysis\)](#)
- [Offline Log Bundle Based Analysis](#)
- [Summary of Supported Products, Analysis Mode, and Checks Available](#)
- [Interacting with the VMware Skyline Health Diagnostics using REST API](#)
- [Working with Analysis Reports](#)
- [Registering VMware Skyline Health Diagnostics Plug-in with VMware vCenter Server](#)
- [Help and Support](#)
- [View the CEIP Data Collected for Reporting and Analytics](#)

## Log in to VMware Skyline Health Diagnostics from Web Browsers

VMware Skyline Health Diagnostics provides a user interface to log in, upload and analyze the log bundles or directly connect to the problematic environment run the diagnostics and other scans. User can also use the web interface for scheduling the periodic checks on their environment. Web interface can also be used for configuration, password, user management, downloading and performing the updates of the VMware Skyline Health Diagnostics.

### Prerequisites

- Verify that you have a compatible web browser installed on your computer.
- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

## Procedure

- 1 Open the web browser and enter the address of the VMware Skyline Health Diagnostics instance. For Example **https://FQDN\_OR\_IP\_ADDRESS\_OF\_VMwareSkylineHealthDiagnostics**.
- 2 If a warning message about un-trusted SSL certificate appears, select the appropriate action based on your security policy.
- 3 Enter the credentials of the user and click on the **Log in** button.
- 4 If the credentials are accepted, you will be redirected to the home page.
- 5 To log out, click the **Log Out** option on the top right corner of the user interface.

## What to do next

Upload a log bundle or zip of multiple log bundles, connect, and analyze any environment, view historical analysis reports. Manage the configurations, updates of new features and plug-in, signatures of the VMware Skyline Health Diagnostics.

# Operations in the VMware Skyline Health Diagnostics

You can upload, analyze, run security, health, pre-upgrade, drivers, and hardware scans periodically and view or get email notifications of the reports using the VMware Skyline Health Diagnostics. The intent base analysis has been introduced to provide more flexibility to product administrators. Now, you can select the product and related workflows that are more aligned with your intent and operations.

## Operations

The VMware Skyline Health Diagnostics support below operations,

- Run Diagnostics, VMware Security Advisory Scan, Health Checks, Pre-upgrade checks, and assessment, and VMware Compatibility Guide Checks, for details on supported checks and VMware products refer to section [Summary of Supported Products, Analysis Mode, and Checks Available](#)
- Upload log bundles from local or remote server and run the analysis for details on supported checks and VMware products refer to section [Chapter 6 Supported Versions and Compatibilities](#)
- View results of the analysis in the form of reports.
- View and download the past analysis details reports.
- Schedule periodic Health, Security, and Hardware Compatibility scans and get the reports to your mailbox.

## Browsers Supported

Operating System	Browser
Windows 10	Microsoft Internet Explorer 11 and later. Mozilla Firefox: 56 and later. Microsoft Edge: 44.18362.449.0. Microsoft Edge HTML: 18.18363 and later Google Chrome: 84 and later. Safari: 12.1 and later.
Mac OS	Mozilla Firefox: 56 and later. Google Chrome: 84 and later. Safari: 12.1 and later.

## Direct Connect and Analyze (Live or Online Analysis)

You can use this option to perform live analysis on an environment in which the problem has occurred or you want to run or schedule available diagnostics checks to proactively monitor the environment. The VMware Skyline Health Diagnostics will require set of details about the environment, post which it will connect to it, collect the required data, run the analysis, and generate the reports with details about findings or current state.

## Working with Analysis Profiles and Schedules

The VMware Skyline Health Diagnostics version 4.0.0 and onwards you can save the inputs provided for the analysis and reuse it as profiles. The profile saves the inputs provided for the analysis like VMware Products to analyze, checks to be performed, connection details, notification, and scheduling details.

For input, details refer to section [Supported Diagnostic Checks for Products and Related Input Requirements as part of Analysis Profile](#)

**Important** If you want to use Notification feature, refer section [Configuring Notification Feature of VMware Skyline Health Diagnostics](#) to know more about configuring Notifications.

### Caution

- 1 You cannot save a profile if it includes checks that cannot be re-run at a later point in time. Example offline diagnostics cannot be saved as profile.
- 2 Similarly, some of the checks cannot be scheduled and hence profiles having such checks cannot be scheduled. Example vSphere Diagnostics checks cannot be scheduled. However, you can still save them as profiles and run manually.
- 3 Exclusive Checks and Non-Exclusive Checks: Some of the checks across the products can appear as exclusive checks. An exclusive check cannot be selected along with other checks. It can be the only check included in the analysis.

## Managing the Credential Store

You can encrypt and secure the inputs such as password, connection details and other inputs required for the analysis of the VMware products using the encryption key and credential store.

### Usage

Credential store is a secure vault which stores all the input parameters provided for the analysis, in encrypted form using AES with Galois or Counter Mode encryption. The key used for the Credential Store must be provided by the VMware Skyline Health Diagnostics user with Administrator role. This key must be kept at the secured location by the users as it is used to encrypt all the data stored for the analysis profiles.

By default Credential Store is turned off and you must enter a valid encryption key to enable it. Every time the VMware Skyline Health Diagnostics service or appliance is restarted the Credential Store must be enabled manually with the encryption key. Without enabling the Credential Store, you cannot save profiles for later use. If you have enabled the Credential Store, the analysis profiles are encrypted using the encryption keys, and then if appliance restarts, by default Credential Store is deactivated, and the scheduled tasks are paused till the time Credential Store is enabled again.

### Activate the Credential Store

The Credential Store encrypts the input parameters in the analysis profile, and you can enable the encryption store by providing a strong encryption key.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Select the **Scheduler** tab from the top menu, click **Activate Credential Store**.
- 3 Enter a strong Encryption Key to be used with Credential Store.

The key must be of at least twelve characters with one number, one uppercase and lowercase alphabets and one of the special characters like !@#%&\*? .

Maximum supported length for the Encryption Key is Thirty-Two characters.

- 4 Click **Save**.

Once key is saved successfully, the Credential Store will be enabled.

### Results

The Credential Store is enabled, and you can save analysis profiles and use the scheduler feature.

## What to do next

You must remember or keep the key at secured place to refer when needed.

## Deactivate the Credential Store

You can deactivate the Credential Store which will pause the usage of all profiles and scheduled analysis.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 Verify that the **Credential Store** is enabled.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Select the **Scheduler** tab from the top menu, click **Deactivate Credential Store**.

The Credential Store must be deactivated, all the scheduled analysis will be stopped running periodically and notification will not be sent to the subscribed users.

## Activate Credential Store after restarting the Service or Appliance

Credential Store stays deactivated till you re-enter the Encryption Key. So any time the VMware Skyline Health Diagnostics service or the appliance is restarted, you must Activate the Credential Store by entering the Encryption key.

If you restart the `vmware-shd` service or the VMware Skyline Health Diagnostics appliance and log in to the user interface, **Activate Credential Store** button will be enabled under the **Scheduler** tab. This is expected behavior.

After the restart of the `vmware-shd` service or the VMware Skyline Health Diagnostics appliance, the application does not have the Encryption Key with it. The key you have provided is never persisted on the **VMware Skyline Health Diagnostics** appliance. To get the Credential Store activated after the restart, you must provide the Encryption Key that was used when you activated it for the first time.

Follow the steps below to enable and re-run the scheduler.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 Verify that the **Credential Store** was activated at least once in the past.

## Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Select the **Scheduler** tab from the top menu.
- 3 Click **Activate Credential Store**.  
**Enter Passphrase for Key** dialog box is displayed.
- 4 Enter the key that you have provided initially to enable the credential store.
- 5 If the key validation succeeds, then **SAVE** button will be enabled.
- 6 Click **SAVE**.

## Results

The Credential Store must be activated, all the scheduled analysis will resume running periodically and analysis reports will be sent to the subscribed users using notifications.

## Change the Encryption Key for the Credential Store

You can change the Encryption Key periodically as per the organization compliance policy to ensure safety and security of the data.

## Prerequisites

- 1 Verify that you have `root` user credentials for the VMware Skyline Health Diagnostics appliance.
- 2 For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- 3 Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.
- 4 Verify that you have `shd-admin` user credential for the VMware Skyline Health Diagnostics appliance.
- 5 Verify that you have the current and the new Encryption Key for the Credential Store

## Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Run the command `shd-config credmanager`
- 4 Provide Password for `shd-admin` user at the prompt.

- 5 Select the Option number for **Rekey the Credential Store** option, if you know the current encryption key and want to change it.
- 6 Enter the current encryption key.
- 7 Enter the new encryption key you want to set.
- 8 Confirm the new encryption key .
- 9 Once the rekey operation finishes, restart the `vmware-shd` service using command `systemctl restart vmware-shd`.

Time required to complete the re-key operation will vary depending on the number of profiles stored in the Credential Store.

### Results

The encryption key is changed for the Credential Store.

### What to do next

Save the passphrase at the secured place to refer it later.

### Reset the Encryption Key for Credential Store

You can reset the Encryption Key for the Credential Store in case you forget the current encryption key.

### Prerequisites

- 1 Verify that you have `root` user credentials for VMware Skyline Health Diagnostics appliance.
- 2 For more information about enabling the `root` user log in to the VMware Photon OS, see: [https://vmware.github.io/Photon/assets/files/html/3.0/Photon\\_troubleshoot/permitting-root-login-with-ssh.html](https://vmware.github.io/Photon/assets/files/html/3.0/Photon_troubleshoot/permitting-root-login-with-ssh.html) (This configuration is not necessary for the VMware Skyline Health Diagnostics appliance as by default it is configured to allow root user log in through SSH).
- 3 Verify that you can log in using `root` credentials to the VMware Skyline Health Diagnostics appliance console.
- 4 Verify that you have `shd-admin` user credential for the VMware Skyline Health Diagnostics appliance.

---

**Caution** Resetting the Encryption key will invalidate in all the saved Analysis Profiles and Schedules. You will have to delete them and recreate once the Credential Store is reset.

---

### Procedure

- 1 Open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 2 Log in as `root` user.
- 3 Run the command `shd-config credmanager`

- 4 Provide **shd-admin** credentials as requested.
- 5 Select the option for **Re-Initialize the Credential Store**.
- 6 Enter the **new** passphrase you want to set.
- 7 Confirm the new passphrase you want to set.
- 8 Once the reset operation completes, restart the **vmware-shd** service using command **systemctl restart vmware-shd**.

## Results

The new passphrase is set for the **Scheduler** of the VMware Skyline Health Diagnostics Appliance.

## What to do next

You must delete the existing Analysis Profiles and re-create them as the existing profiles are stored after encrypting with old encryption key they cannot be restored.

## Create a New Analysis Profile

You can analyse and get recommendation for the issues impacting the health, availability, hardware compatibility, and reliability of the VMware products using the new analysis. You can also schedule the analysis and configure notifications to receive reports. You can save these inputs for future reuse as profile.

## Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that the **Credential Store** is activated.
- Verify that you have the user credentials for the VMware Products to run the analysis.
- Verify that the required user has roles and permissions to collect logs from the VMware Product.
  - Each of the products may have different Permissions or Role requirement to allow an authenticated user to collect logs. Consult respective product documentation for details.
- Verify that the user account used for VMware product has required privileges to connect through API, collect inventory details and configuration and other related data.
- Some checks will require remote connectivity over SSH Session to the target server. Make sure it is available, and you have access required user credentials.

## Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.



2 In the top menu, click **Analyze > New Analysis**.

3 Select the intended VMware Product to diagnose from the **Select Product to Analyze** on the **Diagnostics Checks** page.

4 Select the diagnostics checks you want to execute and click **Next**.

The input requirement on **Target Details** page will vary depending on the product and checks that you have selected.

5 On **Target Details** page, enter the details as requested by referring to section [Supported Diagnostic Checks for Products and Related Input Requirements as part of Analysis Profile](#).

Include the port for the FQDN or IP address of the VMware product if the service is not running on the standard HTTPS Port (443).

Example: server.doamin.com:8080

6 Click **Connect** to validate the input details and optionally bring up the inventory for selecting further target objects.

- **Connect** action validates the credentials by performing log in to the given VMware product.
- Inventory is displayed only if it is required for the selected checks.
- Displays the product inventory if connection is successful.

7 Select the intended inventory items to diagnose if inventory is displayed and click **Next**.

8 Provide the required details on the **Profile Details** page, refer to instructions in section [Instructions to update the Profile Details page](#)

9 Click **Next** button to review the details on the final **Review** page.

10 Click **Save & Run** to save the profile and start the analysis.

- **Save & Run** is displayed only if you choose to save the analysis profile by providing **Name for the Profile** in **Diagnostics Details** page.
- **Run Without Save!** Is displayed if you choose to keep the **Name for the Profile** field empty in **Diagnostics Details** page.

## Results

Once you have submitted the analysis, details will be validated, and analysis task will start.

In case, validation fails, appropriate error message will appear, and you are requested to navigate back and update the input values to fix the errors.

On successful submission:

- New task entry will appear under **Analyze>Tasks** table.
- If you have chosen to save this profile, the new profile will be created and listed under **Analyze>Profiles** pane.

- On successful completion of the task, analysis report will be generated and listed under **Show Reports** pane.

### Instructions to update the Profile Details page

You can tag the analysis task, save the inputs for the analysis run, and configure notifications to receive the report using diagnostics details page.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that you are not trying to create the new analysis profile and modifying the existing analysis profile.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Analyze**, select the profile from the **Profiles** pane which you want to modify.
- 3 Enter **Name for the Profile** to save this run as analysis profile.  
If you intended to save the profile, enter a name and click **Check For Duplicate** to ensure the name is unique.
- 4 Input the tag name under **Tags** to identify the analysis. The tagging helps in quick search of the analysis report from **Show Reports** section.
- 5 Input the **Limit days** to limit the analysis of logs to the specified number of days from the log collection date.  
If you do not specify any value, default value is **0** to analyze all the logs. Example If you are collection of the logs at July 20th and you want to limit the analysis of log from July 10th till July 20th, then you will input value **10** in the **Limit days**.
- 6 Select **Send Notification** to receive email for the completion status and the report of the analysis.
- 7 Select the applicable **Notification Distribution Group** from the available options. You can select more than one from the existing list.  
**Distribution Group** is mandatory when **Send Notification** is selected.
- 8 Expand **Enter Scheduling Details** section, check **Enable Scheduler** to schedule this analysis at a defined frequency.
  - Scheduling option is available for only certain type of checks.
  - Supported frequencies are Daily, **Weekly**, **Monthly**.

## Results

Profile and other related details are updated.

## Run an Existing Analysis Profile

You can run an existing Analysis Profile to get the report of the issues.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that the **Credential Store** is activated.
- Verify that the credentials stored as part of profile are still valid.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Analyze**.
- 3 Select the profile from the **Profiles** pane which you want to run.
- 4 Click play icon to **Run** the selected profile.
- 5 In the resulting Profile Summary dialog, click **Run** to start the execution of the checks.

## Results

On successful submission:

- New task entry will appear under **Analyze>Tasks** pane.
- On successful completion of the task, analysis report will be generated and listed under **Show Reports** tab.

## Editing an Existing Analysis Profile

You can edit an existing Analysis Profile to change the target details, checks included, update the credentials. You can also change the scheduler and notification related details.

### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.
- Verify that the **Credential Store** is activated.
- The users with *SHD Operator* role can only edit the profiles they have created.
- The users with *SHD Administrator* role can edit any of the profiles.

- All the prerequisites for creating a new profile will apply to edit workflow too.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Analyze**.
- 3 Select the profile from the **Profiles** pane which you want to edit and click **Edit**.  
Edit Profile wizard is displayed.
- 4 On **Diagnostic Checks** page select or de-select the diagnostic checks as required.  
Note: You are not allowed to change **Select Product to Diagnose**.
- 5 Click **Next**.
- 6 On **Target Details** page, update the details as requested, if required.
- 7 Click **Connect** to validate the input details and optionally bring up the Inventory tree for selecting further target objects.  
Note: Inventory is displayed only if it is required for the checks included.
  - **Connect** action validates the credentials by performing log in to the given VMware product.
  - Displays the product inventory if connection is successful.
- 8 Select or modify the intended inventory items to diagnose if the inventory tree is displayed and click **Next**.
- 9 On the **Profile Details** page update the details as required for **Tags**, **Limit days**, **Notification Settings**, and **Schedule Details**.  
**Name for this Profile** is read only in edit mode and cannot be changed.
- 10 Click **Next** button to review the details on the final **Review** page.  
Review Page is displayed with a summary of the Analysis.
- 11 Click **Save**.  
Details will be validated. If validation fails, you are expected to navigate to previous wizard pages and update the input values to address the validation failure.

#### Results

On successful submission, profile values will be updated.

### Remove or Delete Analysis Profile

You can delete a profile when it is no longer needed or become invalid. For example, the VMware product instance is decommissioned, and profile cannot be run anymore.

### Prerequisites

- Verify that you have credentials for VMware Skyline Health Diagnostics user interface.
- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.
- The users with Operator role can only remove the profiles they have created.
- The users with Administrator role can remove any of the profiles.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Analyze**.
- 3 Select the profile you want to delete from **Profiles** pane.
- 4 Click **Remove**.
- 5 Click **Ok** in the delete confirmation dialog box.

### Results

The selected profile is deleted from the profile list.

## Copy an Existing Analysis Profile

You can make a copy of an existing Analysis Profile with a new name.

### Prerequisites

- Verify that you have credentials for VMware Skyline Health Diagnostics user interface.
- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.
- The users with Operator role can only copy the profiles they have created.
- Verify that the **Credential Store** is activated.
- The user with Administrator role can make a copy of any of the profiles.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Analyze**.
- 3 Select the profile you want to duplicate from **Profiles** pane .
- 4 Click **Duplicate**.

5 Enter **New Profile Name**.

6 Click **Validate Name** to validate and avoid the duplicates.

Profile names must be unique. Validation will fail if the provided name is already in used by other profile.

7 Click **Save** to make a copy of the profile.

8 By default scheduling is disabled for such profile, edit the profile to enable the scheduler if needed.

### Results

A copy of the selected profile is created with the new profile name.

---

**Caution** A profile created through duplicate option will always have the scheduling deactivate irrespective of the schedule state of source profile.

---

## Scheduling Analysis Runs

VMware Skyline Health Diagnostics has a scheduler which allows you to run analysis at periodic intervals. Starting version 4.0.0, this feature is integrated with Analysis Profiles.

Refer to the [Working with Analysis Profiles and Schedules](#) section to understand more about Creating or Editing the Schedules.


### Configure the Scheduler Behavior

You can configure the behavior of the scheduler and maximum number of scheduling task that can run in parallel. By default scheduler checks for any pending schedules every ten minutes and tries to run at the max three at a time.


#### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Access the Configuration Settings page. See: [Update the Value of the Configuration Property](#)
- 3 To modify how often scheduler should check for pending schedule tasks, locate **Scheduler Run Frequency** setting.
- 4 Click the edit button  , enter the value and close the dialog box, new value should be saved.

5 To modify the number of parallel scheduled tasks locate **Max Schedule Submit Task** setting.

6 Click the edit button  , enter the value and close the dialog box, new value should be saved.

## Creating a New Schedule

To create a new schedule, you need to create a new profile with Product and Diagnostic Checks you want to be part of the scheduled analysis with run frequency.

### Prerequisites

Refer to the [Working with Analysis Profiles and Schedules](#) section to understand more about Creating or Editing Schedules.

## Modifying the Frequency of the Schedule

You might want to change the frequency of schedule.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 Verify that the **Credential Store** is activated.
- 4 The users with SHD `Operator` role can only edit the scheduled analysis they have created.
- 5 The users with SHD `Administrator` role can edit any of the schedules.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Scheduler**.
- 3 Select the existing schedule you like to modify from the list and click the **Edit Schedule** button.
- 4 Update the schedule setting and **SAVE**.

### Results

The schedule frequency is updated.

## Deleting the Schedule

You can delete the schedule as per your needs.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.

- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 The users with SHD `Operator` role can only delete the scheduled analysis they have created.
- 4 The uses with SHD `Administrator` role can delete any of the schedules.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Scheduler**.
- 3 Select the existing schedule that you want to delete from Schedule table.
- 4 Click **Delete**.

#### Results

Schedule will be deleted from the list.

## Accessing the Report of Scheduled Scan Run

You might want to see the report of the Scheduled Scan Run.

#### Prerequisites

- 1 Verify that you have a valid user account credential with the VMware Skyline Health Diagnostics.
- 2 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 3 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with operator or administrator privilege.
- 2 In the top menu, select **Scheduler**.
- 3 Select the Scheduled Run to view the Report and click the View Report.  
View report is enabled.
- 4 The Report will be displayed to you.

## Supported Diagnostic Checks for Products and Related Input Requirements as part of Analysis Profile

The VMware Skyline Health Diagnostics need various inputs to complete the analysis. These inputs differ based on the VMware product you would like to analyze and checks you select while running the analysis.



## Diagnostic Checks and Input Requirements for vSphere Related Analysis

You can connect and analyze issues for the VMware vCenter Server, VMware ESXi, and VMware vSAN. Depending on the checks that you select, the inputs requirements vary.

Product	Diagnostic Check	Input Requirements	Notes
VMware vSphere	vSphere Diagnostics VMware Security Advisory Scan VMware Compatibility Guide Check for ESXi Servers vSAN Cluster Health Check	<ul style="list-style-type: none"> <li>■ VMware vCenter Server FQDN or IP address</li> <li>■ SSO User Credentials</li> <li>■ Appliance user (root) credentials</li> <li>■ Inventory Selection of hosts and clusters.</li> </ul>	For Disconnected or not responding hosts in the selection, you will need local user (root) SSH credentials for each selected host.  If you save a profile with Disconnected Hosts, the credentials for such hosts are not persisted. Later runs of these profiles will treat the hosts as connected and might fail if the host is not connected back.
VMware vCenter Server	vCenter Server Health Check vCenter Server Upgrade Pre-Check*	<ul style="list-style-type: none"> <li>■ VMware vCenter Server FQDN or IP address</li> <li>■ SSO User Credentials</li> <li>■ Appliance user (root) credentials</li> </ul>	VMware vCenter Server Health Check is supported only on appliance based vCenter Servers.  Appliance root user credentials are optional for vCenter Server Health Check. If they are provided few more checks will be run as part of the analysis.  SSH must to be enabled on the vCenter Server Appliance.
VMware vCenter Server	VMware Security Advisory Scan	<ul style="list-style-type: none"> <li>■ VMware vCenter Server FQDN or IP address</li> <li>■ SSO User credentials</li> </ul>	
VMware vCenter Server Appliance or Platform Service Controller	vCenter Server/PSC Appliance Direct Connect Diagnostics*	<ul style="list-style-type: none"> <li>■ VMware vCenter Server FQDN or IP address</li> <li>■ Appliance user (root) credentials</li> </ul>	Use this mode when the VMware vCenter Server is not accessible over UI or API.
VMware ESXi	Direct Connect Diagnostics. VMware Security Advisor Scan VMware Compatibility Guide Check for ESXi Servers	<ul style="list-style-type: none"> <li>■ VMware ESXi Server FQDN or IP address</li> <li>■ Local user (root) Credentials</li> </ul>	Preferred for VMware ESXi which are not managed by the VMware vCenter Server.

Product	Diagnostic Check	Input Requirements	Notes
VMware vSAN	vSAN Cluster Health Check	<ul style="list-style-type: none"> <li>■ VMware vCenter Server FQDN or IP address</li> <li>■ SSO User credentials</li> <li>■ Selection of Clusters from Inventory</li> </ul>	Cluster selection is optional and if not selecting any cluster will result in running the analysis on all vSAN Enabled clusters found in the inventory of the VMware vCenter Server.
VMware vCenter Cloud Gateway	Direct Connect Diagnostics.	<ul style="list-style-type: none"> <li>■ VMware Cloud Gateway Appliance FQDN or IP address, along with the port (Default is 5480)</li> <li>■ Appliance user (root) credentials</li> </ul>	VMware Cloud Gateway diagnostics is supported by connecting to the appliance and performing the diagnostics using the log bundle.

\*: Exclusive check cannot be used with the other checks available.

## Diagnostic Checks and Input Requirements for VMware Cloud Foundation Related Analysis

You can connect and analyze issues for the VMware Cloud Foundation. Depending on the checks that you select, the inputs requirements vary.

The VMware Cloud Foundation Health Check has checks related to the VMware Cloud Foundation workload and management domains for the products that includes,

- VMware vCenter Server
- VMware ESXi
- VMware NSX
- SDDC Manager
- VMware VxRail Manager
- VxRail Manager
- VMware Aria Automation
- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Suite Lifecycle
- VMware Workspace ONE Access

Product	Diagnostic Checks	Input Requirements	Notes
VMware Cloud Foundation	<ul style="list-style-type: none"> <li>■ VMware Cloud Foundation Upgrade Assessment*</li> <li>■ SDDC Manager Diagnostics</li> </ul>	<ul style="list-style-type: none"> <li>■ SDDC Manager FQDN or IP Address</li> <li>■ SSO User Credentials for SDDC Manager</li> </ul>	
VMware Cloud Foundation	<ul style="list-style-type: none"> <li>■ VMware Security Advisory Scan</li> <li>■ VMware Cloud Foundation Health Check</li> <li>■ VMware Cloud Foundation Verify Checks*</li> </ul>	<ul style="list-style-type: none"> <li>■ SDDC Manager FQDN or IP Address</li> <li>■ SSO User Credentials for SDDC Manager</li> <li>■ SDDC Manager super user credentials</li> </ul>	SSH needs to be enabled on the target SDDC Manager and domain component servers.

\* Exclusive check cannot be used with the other checks available.

## Diagnostic Checks and Input Requirements for VMware Horizon Related Analysis

You can connect and analyze issues for the VMware Horizon Connection Server and Horizon Agent for Windows or Linux using the VMware Skyline Health Diagnostics.

Product	Diagnostic Checks	Input Requirements	Notes
VMware Horizon	Horizon Diagnostics	<ul style="list-style-type: none"> <li>■ Connection Server FQDN or IP address.</li> <li>■ User Credentials for the Connection Server with log collection role.</li> <li>■ An agent search filter to include the agents in the inventory.</li> </ul>	<p>Agent search filter helps you to limit the agent information part of Inventory. You can use wildcard character * to create a search filter.</p> <p>Example agent-domain-a* will select all the agents having names starting with agent-domain-a.</p> <p>This field is optional. Leaving it blank will result in only Connection Servers part of Inventory tree.</p>

## Offline Log Bundle Based Analysis

You can use this option to perform analysis on an existing log bundle of the supported product and version. You can use the local upload or remote file upload feature depending on the location of the log bundle. At run time all applicable checks will be selected automatically without you requiring to specify any.

### Prerequisites

- Verify that you have the log bundle from the [Chapter 6 Supported Versions and Compatibilities](#) for diagnostics.

- The log bundle can be in your local machine or in a remote file server.
- If you want to analyze the log bundle from remote server location, the remote server must be reachable from Skyline Health Diagnostics Server.
- The remote server must support one of these protocols for the file transfer,
- HTTP, HTTPS, FTP, SFTP, or FTPS.

Log Bundle- This is the diagnostic data collected from the [Chapter 6 Supported Versions and Compatibilities](#) using the export system logs option from the product user interface or using the command line option. A single log bundle can contain diagnostic data from multiple VMware ESXi hosts and the VMware vCenter Servers. You can also use the support log bundles collected during installation failure of VMware ESXi or VMware vCenter Server.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface using the supported web browser.
- 2 In the top-menu, click **Analyze** tab.
- 3 Click **Log Bundle Analysis**.
- 4 Choose **Local File** or **Remote File** on **Log Bundle** page and click **Next**.  
**Target Details** page is displayed.
- 5 For the **Local file** selection:
  - a Click **Browse** to select the log bundle to be analyzed and click **Open**.
  - b Click **Next**.  
**Profile Details** page is displayed.
- 6 For the **Remote file** selection:
  - a Click **Next**.  
**Enter Target Details** page is displayed.
  - b Select **File Server Protocol**
  - c Provide the remote file server FQDN or IP address in **File Server Address/Host Name**
  - d Provide the location of file in **Path to the file on the File Server** field.
  - e `/<dir1>/<dir2>/<file_name>`.
  - f Provide the **Username** and **Password** for authenticating to File Server if required for the remote server.
  - g Click **Next**.  
**Profile Details** page is displayed.

- 7 Provide the required details on the **Profile Details** page, refer to instructions in section [Instructions to update the Profile Details page](#)

Note:

- Log Bundle analysis cannot be saved as profile.
- Log Bundle analysis cannot be scheduled.

- 8 Click **Next**.

The **Review** page displays all the inputs you have provided.

- 9 Review all the field values and click **Run**.

## Results

On successful submission,

- For local file upload, **Upload progress** bar will be displayed.
- New task entry will be created under **Analyze>Tasks** status table.
- On successful task completion analysis report will be generated and listed under **Show Reports** section.

## Summary of Supported Products, Analysis Mode, and Checks Available

The VMware Skyline Health Diagnostics supports two modes of analysis runs. You can use the **Connect and Analyze** method to perform live analysis and **Upload Log Bundle** for the offline analysis by uploading the log bundles of the target server running supported product and version.

### Products Supported with different Analysis Modes and plug-in allowed to run.

Product	Mode of Analysis	Supported Checks	Notes
VMware vCenter Server	Connect and Analyze (Live/Online Analysis)	<ul style="list-style-type: none"> <li>■ Diagnostics</li> <li>■ VMware Security Advisory (VMSA).</li> <li>■ Health Checks.</li> <li>■ Upgrade Pre-checks.</li> </ul>	General Support.
VMware vCenter Server	Upload Log Bundle.	<ul style="list-style-type: none"> <li>■ Diagnostics</li> <li>■ VMware Security Advisory (VMSA)</li> </ul>	General Support
VMware ESXi	Connect and Analyze (Live/Online Analysis)	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> <li>■ VMware Security Advisory (VMSA).</li> <li>■ VCG (VMware Compatibility Guide).</li> </ul>	General Support.

Product	Mode of Analysis	Supported Checks	Notes
VMware ESXi	Upload Log Bundle.	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> <li>■ VMware Security Advisory (VMSA).</li> <li>■ VCG (VMware Compatibility Guide).</li> </ul>	General Support.
VMware vSAN	Connect and Analyze (Live/Online Analysis)	<ul style="list-style-type: none"> <li>■ Health Checks.</li> </ul>	General Support.
VMware Cloud Foundation	Connect and Analyze (Live/Online Analysis)	<ul style="list-style-type: none"> <li>■ SDDC Manager Diagnostics.</li> <li>■ Health Checks.</li> <li>■ VMware Security Advisory (VMSA).</li> <li>■ Upgrade Assessment.</li> </ul>	General Support.
VMware Cloud Foundation	Upload Log Bundle.	<ul style="list-style-type: none"> <li>■ SDDC Manager Diagnostics.</li> <li>■ VMware Security Advisory (VMSA).</li> </ul>	General Support.
VMware Horizon	Connect and Analyze (Live/Online Analysis)	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> </ul>	General Support.
VMware Horizon	Upload Log Bundle.	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> </ul>	General Support.
VMware SD-WAN	Upload Log Bundle.	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> </ul>	Tech Preview.
VMware vCenter Cloud Gateway	Upload Log Bundle	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> </ul>	Tech Preview.
VMware vCenter Cloud Gateway	Connect and Analyze (Live/Online Analysis)	<ul style="list-style-type: none"> <li>■ Diagnostics.</li> </ul>	Tech Preview.

## Interacting with the VMware Skyline Health Diagnostics using REST API

The **VMware Skyline Health Diagnostics** provides rich set of REST APIs using which you can Configure, Manage and Operate Analysis related tasks. These are documented using OpenAPI Specification, Version 3.0 and available as part of the deployment.

### Authenticating with the VMware Skyline Health Diagnostics REST API Server

REST APIs use JWT based authentication tokens and they are passed with each request using header option `Authentication` with value `Bearer JWT_Token` where `JWT_Token` is the `access_token` obtained using `Token Request` API.

The token request API expects a valid credential of **VMware Skyline Health Diagnostics** user. On successful authentication, The **VMware Skyline Health Diagnostics** REST API Server will return two types of JWT Tokens.

- *access\_token*: A short lived JWT token to be used in header for all protected endpoint on the **VMware Skyline Health Diagnostics** REST API Server
- *refresh\_token*: A long lived JWT Token to be used to refresh the *access\_token* either before or after the expiry of current *access\_token*.

Token expiry time will be part of the response received for Token Request/Refresh request.

Some of the APIs can be used only by a user with *SHD Administrator* role. These endpoints will return `HTTP Error 403` when accessed by a user without *SHD Administrator* role.

## Using the API Explorer

API Explorer provides a swagger-based interface using which you can explore the REST APIs for **VMware Skyline Health Diagnostics**. The API Explorer is hosted along with the user interface and can be accessed from the **VMware Skyline Health Diagnostics** user interface by navigating to **Right Menu Options > API Explorer** or using the direct link `https://<appliance_ip_or_hostname>/api/apischema/swagger`. You can download the JSON Schema using link `https://<appliance_ip_or_hostname>/api/apischema`

Though the API Explorer doesn't need any credentials to access, you will need a valid login credentials for the **VMware Skyline Health Diagnostics** to be able to use or try out the APIs.

## Summary of available REST APIs

API Explorer organizes all available APIs using Tags. These tags are logical grouping of available APIs based on the area of application or operation of these APIs.

This table provides a summary of all the APIs and related actions you can perform using REST APIs. Use the API Explorer to review detailed documentation about the APIs.

Tag	Description	Actions	Notes
Authentication	APIs related to authenticating to the <b>VMware Skyline Health Diagnostics</b> .	Request, Refresh or Delete (logout) token from <b>VMware Skyline Health Diagnostics</b> Server.	
Credential Store	Manage the Credential Store.	Activate/Deactivate and check the Status of Credential Store.	

Tag	Description	Actions	Notes
Trust Manager	Manage the Trust information of the Targets SHD is expected to connect.	Add/Remove trusted targets to/from trust store.	By default, <b>VMware Skyline Health Diagnostics</b> doesn't connect to any Target whose certificate cannot be verified. You need to explicitly trust them by adding information to trust store.
Management	Configure and manage the <b>VMware Skyline Health Diagnostics</b>	Configure License and CEIP settings, Manage SMTP/Distribution Groups, Manage Proxy Settings, Update VCG Database, User Management, Update Management.	
Workflow Common	Common operations related to Analysis workflow and Profiles.	Retrieve a list of supported products and available checks, List, Run or Delete available profiles.	Create, Edit and Copy Profile APIs are not available with this release. Use the user interface to perform the operation.
Workflow Report	Report Management.	Retrieve HTML/Binary reports for the Analysis.	Binary reports are gzipped HTML Reports which are Base64 encoded. As the reports content can be quite large, it is advised to use Binary option over the HTML option.
Workflow Summary	Summary of Analysis Workflow/Run.	Get Summary of Analysis, Tasks, Delete an analysis record.	
Tasks	Task Management	Retrieve Status, Summary of Analysis tasks.	
VMware vSphere Workflows, VMware vCenter Server Workflows VMware ESXi Server Workflows VMware vSAN Workflows	Analysis related actions for Analysis or Diagnostics of VMware vSphere Products.	Retrieve available checks, Validate/Start new Analysis Workflow/Run.	A new target with Self Signed or non-verifiable certificate needs to be added to trust store before it could be analyzed.
VMware Cloud Foundation Workflows	Analysis related actions for Analysis/Diagnostics of VMware Cloud Foundation.	Retrieve available checks and Validate/Start new Analysis Workflow/Run.	A new target with Self-signed or non-verifiable certificate needs to be added to trust store before it could be analyzed.



Tag	Description	Actions	Notes
VMware Horizon Workflows	Analysis related actions for Analysis/Diagnostics of VMware Horizon Products.	Retrieve available checks, Validate/Start new Analysis Workflow/Run.	A new target with Self Signed or non-verifiable certificate needs to be added to trust store before it could be analyzed.
Offline	Manage Offline Analysis using log bundles.	Offline Analysis using Local or Remote Log bundles from supported products.	

## Working with Analysis Reports

The VMware Skyline Health Diagnostics creates report for each of the Analysis Run. These reports are available under **Show Reports** section of the UI. These reports provide a consolidated summary and findings of all checks included for each of the target part of the analysis.

### View Analysis Reports in VMware Skyline Health Diagnostics

After the VMware Skyline Health Diagnostics analyzes a log bundle or a product target it generates a detailed report with all findings. You can immediately see it or save it for a later use.

As an **SHD Operator** or **SHD Administrator**, you might want to view the analysis report or compare the recent report with previous report.

#### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using **SHD Operator** or **SHD Administrator** privilege user.
- 2 Click the **Show Reports** tab from the top-menu.
- 3 Click the expand button




to expand the **All reports** menu.


- 4 Select any one option from left-menu. For example,
  - **VSphere Diagnostics**: Lists the reports that have diagnostics plug-in selected at the time of analysis.

- **VCenter Server Upgrade Pre-Check:** Lists the reports that have Upgrade Pre-check plug-in selected at the time of analysis.
  - **VMware Security Advisory Scan:** Lists the reports that have security plug-in selected at the time of analysis.
  - **vSAN Cluster Health Check:** Lists the reports that have vSAN plug-in selected at the time of analysis.
  - **VMware Compatibility Guide Check for ESXi Servers:** Lists the reports that have VCG plug-in selected at the time of analysis.
  - **VMware Cloud Foundation Health Check:** Lists the reports that have VMware Cloud Foundation plug-in selected at the time of analysis.
  - **VMware Cloud Foundation Upgrade Assessment:** Lists the reports that have VMware Cloud Foundation Upgrade Assessment plug-in category selected at the time of analysis.
- 5 Select a log bundle using the filter against the **Bundle Name** , **Analysis Type** , **Tags**, **Username** or **Start Time**. You can use the **Tags** to quickly search the issues base on the keyword that you provided while starting the analysis.



- 6 Click view button  in the right most column to see the details of the report.



- 7 To download the report , click save button  in the right most column.
- a You may want to download only the specific category of report so that you can share it with your respective team. Select respective category or all.
  - b For example,
    1. vSphere Diagnostics.
    2. VMware Security Advisory Scan.
    3. vSAN Cluster Health Check.
  - c Click **Save as HTML** or **Save as JSON**.
- 8 To view the details of report in the same window, click >> icon available on left side of the bundle selected.

## Results

Selected report is downloaded locally or opened in a new window depending on the action.

---

**Caution** You have to enable and allow the pop up in the browser for the VMware Skyline Health Diagnostics user interface to allow the reports download or else it will fail.

---

## Delete Analysis Report in the VMware Skyline Health Diagnostics

In default configuration all analysis reports are saved perpetually. You can configure a default retention period or manually delete the reports. This feature is available from the VMware Skyline Health Diagnostics version 2.5.0 or later. An operator can delete the analysis reports created by self. Admin user can delete analysis reports created by any user.

Deleting Analysis Report.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

---

**Caution** The delete report action is irreversible. Deleted reports are not recoverable.

---

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using **SHD Operator** or **SHD Administrator** privilege user.
- 2 Click the **Show Reports** tab from the top-menu.



- 3 Click the expand button to expand the **All reports** menu.
- 4 Select the report you want to delete.



- 5 Click the delete button in the **Actions** column of the report display row.
- 6 In the confirmation dialog box, click **OK** to delete the report.

### Results

Report is successfully deleted.

## Save or Delete Multiple Analysis Reports

You can select multiple reports and choose one of the actions from Delete or Save for selected reports.

As an operator, you might want to compare the before and after a remediation the resolution status of the issue.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.

- 2 Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

---

**Caution** The delete report action is irreversible. Deleted reports are not recoverable.

---

#### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using **SHD Operator** or **SHD Administrator** privilege user.
- 2 Click **Show Reports** tab from the top-menu.



- 3 Click the expand all button to expand the **All reports** menu.
- 4 Select the reports you want to Delete or Save using the check box in the first column.
- 5 Option to delete or save gets enabled.



- 6 Choose the action you want to perform.
  - a If you want to download all selected reports to your Workstation, click `Save Multiple Bundles`.
  - b If you want to delete all selected reports, click `Delete Multiple Bundles`.
  - c Click `Proceed` in the confirmation dialog box.

#### Results

Selected reports are either saved or deleted depending on the action.

---

**Caution** You have to enable and allow the pop up in the browser for the VMware Skyline Health Diagnostics user interface to allow the reports download or else it will fail.

---


## Configuring Auto Delete for Analysis Reports

In default configuration all the Analysis Reports are saved perpetually. You can configure automatic deletion of past reports after a fixed retention period using the configuration option.

#### Prerequisites

- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.

## Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click the **Settings** tab from the top-menu.
- 3 In the left pane, select **Configuration**.
- 4 Select the property **Report Retention Period** to modify.
- 5 Click the edit button  to update the property value.
- 6 You can directly input the desired value or use the up or down arrow to increment or decrement the value.
- 7 Click **OK** button to save the value.

## Results

Auto deletion of analysis reports is enabled. Reports will be deleted automatically post the configured retention period.

# Interpret the Diagnostics Report of the VMware Skyline Health Diagnostics

Diagnostics report contains multiple sections with a hierarchical summary of analysis and findings.

## View a Summary of Detected Issues

A bundle level report contains multiple sections depending on the types of plug-in selected for the diagnostics run.

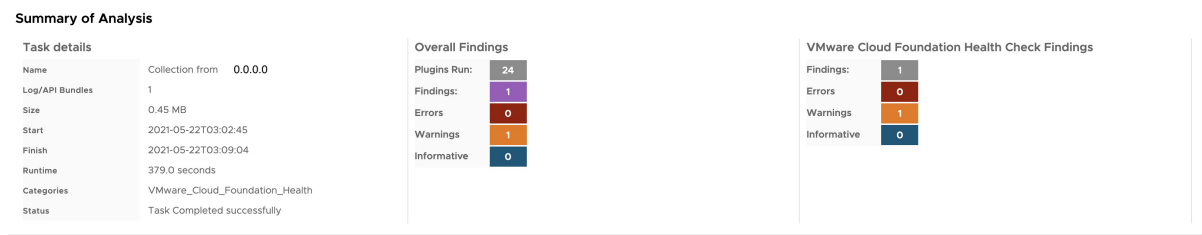
- 1 First section provides a summary of task and findings.

### a Figure 3-1. VMware vSphere Report Summary

Summary of Analysis		VMSA Findings		Diagnostics Findings		vSAN Cluster Health Check Findings	
Task details		Findings:	747	Findings:	103	Findings:	5
Name	Collection from 0.0.0.0	Critical:	196	Errors:	26	Errors:	1
Log/API Bundles	28	Important:	370	Warning:	34	Warnings:	3
Size	12274.45 MB	Moderate:	155	Informative:	43	Informative:	1
Start	2021-09-03T04:13:49	Low:	26				
Finish	2021-09-03T05:25:08						
Runtime	4279.0 seconds						
Categories	DIAGNOSTICS,VMSA_SCAN,VSAN_SCAN						
Status	Task Completed successfully						

- b VMware Cloud Foundation Summary report will display VMware Cloud Foundation related finding.

Figure 3-2. VMware Cloud Foundation Report Summary



- 2 Second optional section provides the summary of VMware Security Advisory Scan if the VMware Security Advisory Scan was selected during the diagnostics runs.

#### Summary of VMware Security Advisory Scanning

- **Critical** (1 findings from 1 advisories across 1 targets)
- **Important**(0 findings)
- **Moderate** (2 findings from 2 advisories across 1 targets)
- **Low**(0 findings)

a

- b The VMware Security Advisory related plug-in is grouped based on published severity level in the advisory.

- 3 Third Section lists all the findings across all the target ESXi hosts/vCenter included in this run. Each analyzed ESXi host/vCenter has a separate section showing all the findings across the selected plug-in types.

All Findings		
Host Name/Log Bundle	Findings	Product/Version
hostname.domain-name.com	Errors <b>12</b> Warnings <b>25</b> Info <b>6</b>	VMware ESXi 6.7.0-build-8169922

#### Summary of Analysis - Task Details

The task details, from the Summary of Analysis section, displays following.

- The details on the analysis task including number of log bundles/hosts.
- Start or end time of the task.
- The total size of all log bundles processed.
- The task status.

## Summary of Analysis

### Task details

<b>Name</b>	Collection from	0.0.0.0
<b>Log/API Bundles</b>	28	
<b>Size</b>	12274.45 MB	
<b>Start</b>	2021-09-03T04:13:49	
<b>Finish</b>	2021-09-03T05:25:08	
<b>Runtime</b>	4279.0 seconds	
<b>Categories</b>	DIAGNOSTICS,VMSA_SCAN,VSAN_SCAN	
<b>Status</b>	Task Completed successfully	

## Summary of Analysis - Findings

These finding cards provide category wise details on number of plug-in run and findings based on the alert or severity levels.

Figure 3-3.

Summary of Analysis											
Task details			VMSA Findings			Diagnostics Findings			vSAN Cluster Health Check Findings		
Name	Collection from	0.0.0.0	Findings:	747		Findings:	103		Findings:	5	
Log/API Bundles	28		Critical:	196		Errors:	26		Errors:	1	
Size	12274.45 MB		Important:	370		Warning:	34		Warnings:	3	
Start	2021-09-03T04:13:49		Moderate:	155		Informative:	43		Informative:	1	
Finish	2021-09-03T05:25:08		Low:	26							
Runtime	4279.0 seconds										
Categories	DIAGNOSTICS,VMSA_SCAN,VSAN_SCAN										
Status	Task Completed successfully										

Depending on the types of plug-in selected, more cards are show with results from those set of plug-in.

**Diagnostics findings** are categorized based on plug-in alert Levels (Error/Warning/Informative)


**VMSA findings** are categorized based on Severity levels of advisory.

**vSAN Cluster Findings** are categorized based on plug-in alert Levels (Error/Warning/Informative)

**VMware Cloud Foundation Findings** are categorized based on plug-in alert Levels (Error/Warning/Informative)

## Summary of VMware Security Advisory Scan

In this section of the report, you find the results from VMware Security Advisory Scan grouped

by the advisory severity. To expand each severity section, click down arrow button . Under each section, all the findings are listed with the list of applicable VMware vCenter Server or VMware ESXi hosts.

## Summary of VMware Security Advisory Scanning

▼ **Critical** (1 findings from 1 advisories across 1 targets)

▼ **VMsa-2021-0002 VMsa-2021-0002.a: VMware vCenter Server - VMware vCenter Server updates address remote code execution vulnerability in the vSphere Client (CVE-2021-21972)**

Target Host	Product/Version	Desired Patch/Update (Minimum)
hostname.host.com	VMware vCenter Server Appliance 7.0.0-15952498	VMware vCenter Server/Appliance 7.0.1: Update 1c

➤ **Important**(0 findings)

➤ **Moderate** (2 findings from 2 advisories across 1 targets)

➤ **Low**(0 findings)


You can click the title of each finding to navigate to the published VMware Security Advisory.

## All Findings

In this section, for each of the host or log bundle analyzed, you find one row with the log bundle or host name, number of findings and product version details.

Summary of each Host/Log Bundle		
Host Name/Log Bundle	Findings	Product/Version
localhost.	Info 0 Warnings 0 Errors 6	VMware ESXi 6.7.0-build-14320388

To expand and view details of the findings, click row expand button  at the start of the row.

Clicking expands all rows button  listed on this section. You can click the same button again to collapse the expanded section.

localhost.

Info 0

Warnings 0

Errors 6

VMware ESXi 6.7.0-build-14320388

Log Directory: esx-localhost-2020-08-02--15.30-2103419

Hostname: localhost. Log Date: 2020-08-02T15:30:06

VMware ESXi 6.7.0-build-14320388 (ESXi 6.7 Update 3 released on 2019-08-20)

Plugins Run 15

Number of Findings 0

Informative 0

Warnings 0

Errors 6

VCG/vSAN HCL Validation Summary

<input checked="" type="checkbox"/>	Device	Description	VCG Status	Driver Status	Current Driver/Version	VCG Driver	Current Firmware	VCG Firmware	Forward Support
<input checked="" type="checkbox"/>	Server	HPE ProLiant DL380 Gen10	<input checked="" type="checkbox"/> Supported	N/A	N/A	N/A	U30	HPE U30_2.22 UEFI Mode (Boot Mode:UEFI)	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmnic0	NetXtreme BCM5719 Gigabit Ethernet (network)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmnic1	NetXtreme BCM5719 Gigabit Ethernet (network)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmnic2	NetXtreme BCM5719 Gigabit Ethernet (network)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmnic3	NetXtreme BCM5719 Gigabit Ethernet (network)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Supported	ntg3 4.1.3.2-1vmw.670.128.10302608	4.1.3.2-1vmw	1.46	N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmnic4	82599 10 Gigabit Dual Port Network Connection (network)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Not Latest	ixgben 1.7.15-1OEM.670.0.0.8169922	1.8.7	0x8000091d	N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmnic5	82599 10 Gigabit Dual Port Network Connection (network)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Not Latest	ixgben 1.7.15-1OEM.670.0.0.8169922	1.8.7	0x8000091d	N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmhba0	Lewisburg SATA AHCI Controller (sata)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Supported	vmw_ahci 12.8-1vmw.670.3.73.14320388	12.8-1vmw		N/A	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmhba1	HPE P408i-a SR Gen10 (sas)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Not Latest	smartpqi 1.0.3.2309-1OEM.670.0.0.8169922	1.0.4.3017	1.99	2.92-[0]	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmhba2	QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter (fc)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Not Latest	qlnativefc 3.116.1-1OEM.670.0.0.8169922	3.131.0-1	8.08.220	8.08.xx	6.7 U3, 7.0
<input checked="" type="checkbox"/>	vmhba3	QLE2692 Dual Port 16Gb Fibre Channel to PCIe Adapter (fc)	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Not Latest	qlnativefc 3.116.1-1OEM.670.0.0.8169922	3.131.0-1	8.08.220	8.08.xx	6.7 U3, 7.0

\*\*Devices used for vSAN are checked against vSAN HCL. vSAN HCL check is currently limited only for the Storage IO Device

#Firmware and BIOS versions are not validated. Please review the details for compatibility

\*\*Devices used for vSAN are checked against vSAN HCL. vSAN HCL check is currently limited only for the Storage IO Device  
 #Firmware and BIOS versions are not validated. Please review the details for compatibility

## Plug-in Summary

For each of findings against the log bundles, you find a comprehensive report outlining the findings, alert level, resolution, investigation details, and log evidence if available. If any knowledge base article is to be associated with the finding, it is included in this section.



**i Storage.SlowStorageOperations: Possible storage bottleneck detected - slow storage operations**

Fix Available In: Please review the environment

**Resolution:**

Some possible Symptoms:

- Tasks failing/timing-out on the host. E.g. vMotion/snapshot/maintenance-mode/vm-power-on.
- Host disconnects from vCenter as soon as you start one of the above tasks.
- ESXi Embedded Host Client is not accessible.
- esxcli commands unresponsive.

Please check for storage issues including HBA, fabric and backend storage

**Evidences from Logs:****Description:** Slowness for Storage operations reported by hostd.**Log File Name:** var/run/log/hostd.log

```
2020-08-02T15:15:19.094Z warning hostd[2099811] [Originator@6876 sub=IoTracker] In thread 2099224,
open("/vmfs/volumes/5dcd5f45-f6e57b6a-cccc-bbbbbbbbbb/VMA_1/VMA_1.vmx") took over 11 sec.
2020-08-02T15:15:19.094Z warning hostd[2099811] [Originator@6876 sub=IoTracker] In thread 2099076,
open("/vmfs/volumes/5dcd5f45-f6e57b6a-cccc-bbbbbbbbbb/VMA_2/VMA_2") took over 11 sec.
```

The title provides a brief description of the issues identified and is colored based on the severity of the finding.

Error NN:- Indicates the issues detected with an error log level. These require immediate attention and user must follow the resolution details provided by the plug-in.

Warning NN:- Indicated the issues detected with a warning log level. Warning plug-in provide the recommendation to avoid a probable issue that might occur in future (For example, multi-path configuration, Unreachable Syslog Targets).

Info NN:- Indicated the issues detected with an info log level. Informational plug-in does not represent any functional issues. They just indicate helpful information from the logs (For example, Host Configuration, BIOS details and, so on).

Below the title, you see the knowledge base article number associated with this finding and the availability of the fix available.

Apart from the title section, a plug-in has one or more of following sections,

- **Resolution:** This section provides more context about the issue identified with the resolution path. A resolution path can be in the form of a patch or an upgrade and configuration changes. If a patch or an upgrade is not available, it lists workarounds available for immediate use.
- **Investigation Details:** This section lists some of the information identified from the logs that provide contextual or companion data related to the identified issues.
- **Evidence from Logs:** This section lists the log statements used for identifying the root cause with the log filename in which they are found. This helps in validating the findings.
- **Back-trace:** This section displays the stack trace from the ESXi host that crashed.

## Interpret VCG or vSAN HCL Validation Summary

Diagnostics report includes detailed report related to hardware compatibility checks performed on the server or IO Devices for the ESXi server for which the log bundle has been analyzed.

### VCG or vSAN HCL Validation

Server and Storage or Network IO devices are validated against the **VMware Compatibility Guides**. vSAN used Storage I/O devices are validated against the **vSAN HCL**. Currently vSAN validation is limited to Storage I/O devices only. Firmware levels for Server and I/O devices are not validated but included in the report.

### VCG or vSAN HCL Validation Summary

This section has a data grid showing one row of each of the findings. Each row shows the device and validation summary.

#### Columns


- Device: Name of the device as it named on ESXi server.
- Description: Description of the device.
- VCG Status: Compatibility Status for the Device.
- Driver Status: Compatibility Status of the Driver being used.
- Current Driver/Version: Driver and the Version being used.
- VCG Driver: The latest driver version as indicated by the VMware Compatability Guide.
- Current Firmware: Firmware currently being used (May not be available for all devices).
- VCG Firmware: Latest firmware version as indicated by VMware Compatability Guide.
- Forward Support: Future upgrade support (Shows current and later versions supported for this device)

#### Status Indicators

- Not Checked: Device was not checked for compatibility as VCG Database is not updated.
- Not Listed: This device was not found on the compatibility guide.
- Supported: Device is supported for the current version of ESXi running.
- Not Supported: Device is NOT supported for the current version of ESXi running.
- Not Latest: Device currently being used is not the latest one compared to the one listed on VCG.
- Not Minium: Driver currently being used is does not meet the minimum version listed on VCG.

## VCG Details

Each row in the VCG or vSAN HCL report can be expanded to view further details from the

compatibility guide. Click expand row button  to expand the row and view the details. Clicking the same collapses, the details section.

## Interpret VMware Cloud Foundation Health Checks Report

The VMware Cloud Foundation Health Check report includes detailed information related to VMware Cloud Foundation Health checks performed on all components of the management and workload domains. It can also perform vCenter and vSAN Cluster Health checks.

### VMware Cloud Foundation Health Check Report

The VMware Cloud Foundation Health Check report displays results of health checks performed on following products that includes,

- VMware vCenter Server
- VMware ESXi Server
- VMware NSX-T
- SDDC Manager
- VxRail Manager
- VMware Aria Automation \*
- VMware Aria Operations \*
- VMware Aria Operations for Logs \*
- VMware Aria Suite Lifecycle \*
- VMware Workspace ONE Access \*

\*Limited Checks available as of 4.0.0

#### VMware Cloud Foundation Health Check Summary

The **Summary of Analysis** section provides following details,

- Category Name - SDDC Health
- Findings - Total number of checks executed.
- Red - Number of checks reporting health status as unhealthy.
- Yellow - Number of checks reporting health status as warning.
- Green - Number of checks reporting health status as healthy.
- Gray - Number of checks reporting unknown status due to data collection failure.

The **Summary of VMware Cloud Foundation Health Check** section provides summary based on the criticality of the health issue. Health issues are categorized into.

- Red - Number of checks reporting health status as unhealthy.
- Yellow - Number of checks reporting health status as warning.
- Green - Number of checks reporting health status as healthy.
- Gray - Number of checks reporting unknown status due to data collection failure.

The **All Findings** section provides access to detailed report, with all the categories selected.

- VMSA\_SCAN - VMware Security Advisory Scans.
- SDDC\_HEALTH - VMware Cloud Foundation Health Check
- VSAN\_SCAN - VMware vSAN Health Check
- VC\_HEALTH - VMware vCenter Server Health Check
- NSX\_CHECK - VMware NSX-T Checks

## VMware Cloud Foundation Health Check Report Details

This section has a data grid showing one row of each of the findings. Each row shows the issues and cause summary with host details.

The **Health Checker** includes following categories:

- 1 Services Health
- 2 NTP Health
- 3 General Health
- 4 Certificate Health
- 5 Password Health
- 6 Connectivity Health
- 7 Compute Health
- 8 Storage Health
- 9 DNS Health
- 10 Composability Health
- 11 Hardware Compatibility Health
- 12 Hosts IPs
- 13 Inventory Info

## Interpret VMware vSAN Storage Report

A diagnostics report includes detailed information related to VMware vSAN Storage Health checks performed on the vSAN enabled clusters in the VMware vCenter Server.

## VMware vSAN Storage Health Diagnostics

VMware vSAN Storage Health Check diagnostics report displays the information for all vSAN enabled clusters selected.

### VMware vSAN Storage Health Summary

The **Summary** section provides following details,

- Plug-in Run
- Number of findings
- Errors
- Warnings
- Informative

The **Analysis Result** section provides summary base on the criticality of the health issue. Health issues are categorized into,

- Error
- Warning
- Info

### VMware vSAN Storage Health Details

This section has a data grid showing one row of each of the findings. Each row shows the Issues and cause summary with host details.

The **Health Checker** includes vSAN Health category. It provides following details,

- 1 Issue Summary: The issue detected by vSAN Health Check plug-in.
- 2 Description: Provides description of the issue.
- 3 KB: It is the VMware Knowledge Base article Id that can describe the issue in detail and provide resolution or workaround if available.
- 4 Resolution: KB link for the issue identified.
- 5 Investigation details: Provides investigation details for the analysis done and impacted hosts.

## Interpret the VMware Horizon Report

A diagnostics report includes detailed information related to VMware Horizon. The support for VMware Horizon is in the technical preview mode.

### VMware Horizon Diagnostics

The VMware Horizon diagnostics reports display information for all the Horizon-related issues.

Description of sections in the VMware Horizon diagnostics report.

The **Summary** section provides following details,

- Plug-in Run
- Number of findings
- Errors
- Warnings
- Informative

The **Analysis Result** section provides summary base on the criticality of the health issue. Health issues are categorized into,

- Error
- Warning
- Info

## Interpret the VMware SD-WAN Products report

A VMware SD-WAN product diagnostics report includes detailed information related to VMware SD-WAN Edge or VMware SD-WAN Gateway. The support for VMware SD-WAN Products is in the technical preview mode.

### VMware SD-WAN Products Diagnostics

The VMware SD-WAN products diagnostics reports displays information for all the VMware SD-WAN Edge or VMware SD-WAN Gateway related issues.

Description of sections in the VMware SD-WAN products diagnostics report.

The **Summary** section provides following details,

- Plug-in Run
- Number of findings
- Errors
- Warnings
- Informative

The **Analysis Result** section provides summary base on the criticality of the health issue. Health issues are categorized into,

- Error
- Warning
- Info

## Add and Remove Tags for the Analysis Report

You can add or remove the tag for the report for quick reference and search, post completion of the analysis run.

As an operator, you might want to quickly search the report base on some tags.

### Prerequisites


- Verify that you can access the VMware Skyline Health Diagnostics user interface.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using **SHD Operator** or **SHD Administrator** privilege user.

- 2 Click on the **Show Reports** tab from the top-menu.

You can filter the reports listed using filters available under **All Reports**. These filters are

collapsed by default and can be expanded by clicking button  in the left pane.

- 3 Select any one of the filters that you are interested in.
- 4 Select a log bundle using the filter against the **Bundle Name** , **Category Type** , **Tags**, **Username** or **Start Time**. You can use the **Tags** to quickly search the issues base on the keyword that you provided while starting the analysis.

- 5 Click add button  in the Tags column for the selected report.

- 6 Input the name of the tag and click ok button  .

The tag will be added for the analysis report.

The newly added tag name appears under the Tags Column.

- 7 To remove the tag click the delete button .

### Results

The tag will be deleted for the analysis report.

## Search and view the Analysis Reports

Each successful task such as diagnostic, health, security and upgrade check performed on the VMware Skyline Health Diagnostics generates a report. The list of generated reports can be viewed based on selected criteria or filters.

As an Operator or an Administrator, you might want to quickly search all the reports generated for a specific VMware ESX Host Machine.

## Prerequisites

Make sure you have a valid user account for the VMware Skyline Health Diagnostics.

## Procedure


- 1 Log in to the VMware Skyline Health Diagnostics user interface using the supported browser.
- 2 Click **Show Reports** on the top navigation menu.



- 3 On left menu, click expand button . Click on **All reports**.

- 4 Select a category shown in the left menu.



- 5 You can filter the listed reports using the following fields. Click the filter button  of the respective column and provide the text to search.

- Bundle Name
- Category
- Tags
- User name
- ID
- Start Time

## Registering VMware Skyline Health Diagnostics Plug-in with VMware vCenter Server

The VMware Skyline Health Diagnostics supports VMware vCenter Server plug-in registration from its user interface. After successful plug-in registration, you can trigger the health or diagnostics analysis, monitor the task status, and view the analysis report within the VMware vCenter Server user interface.

### Registration of Plug-in from vSphere Client 80 U1 and onwards

You can register the VMware Skyline Health Diagnostics plug-in with VMware vCenter Server to perform all the VMware Skyline Health Diagnostics operations from vSphere Client.

As an operator, you might want to register the VMware Skyline Health Diagnostics plug-in on vSphere Client as single point for performing Health & Diagnostics and view reports.

## Prerequisites

- VMware vCenter Server version 8.0 U1 and onward.



- You need a valid **vSphere SSO admin** credentials.
- Verify that you can access vSphere Infrastructure with privileges required for creating and interacting with virtual machines.
- Before installing the VMware Skyline Health Diagnostics, you must download the VMware Skyline Health Diagnostics appliance plug-in OVA from the [VMware Customer Connect site](#).

---

**Note** The naming pattern for the plug-in appliance image OVA is `VMware-Skyline-HealthDiagnostics-Appliance-Plugins-<version>-<build>_OVF10.ova` where **version** and **build** are the current available version and build number of the VMware Skyline Health Diagnostics.

The plug-in appliance is pre-configured with required software and settings to run the VMware Skyline Health Diagnostics. The VMware Skyline Health Diagnostics can be deployed in a single step through the vSphere Web Client connected to the VMware vCenter Server.

---

**Caution** The VMware Skyline Health Diagnostics plug-in is only supported for VMware Standalone vCenter Servers.

---

#### Procedure

- 1 Log in to the **vSphere Client** using the supported browser and **SSO credentials**.
- 2 In the top-menu, click **Menu > Skyline Health Diagnostics**.
- 3 The landing page of the VMware Skyline Health Diagnostics Plugin should open.
- 4 Click on the **Go to Skyline Health Diagnostics** beside **Get OVA Files**, to open Download VMware Skyline Health Diagnostics OVA page.
- 5 Click **Download Now** button in front of OVA with name `VMware-Skyline-HealthDiagnostics-Appliance-Plugins-<version>-<build>_OVF10.ova`, to start the OVA download.
- 6 Navigate back to **vSphere Client**, click on **Install Skyline Health Diagnostics**, this should open install OVA wizard in UI.
- 7 Perform the followings steps:
  - a On the **Select an OVF template** page, select Local file, and click **Upload files**.
  - b On the Open dialog page, select the OVA file, click **Open**, and click **Next**.
- 8 On the **Select a name and folder** page, in the **Virtual machine name** text box, enter the name for the VMware Skyline Health Diagnostics virtual appliance. Select the preferred datacenter, or cluster, or host for the virtual machine and click **Next**.
- 9 On the **Select a compute resource** page, select the preferred VMware ESXi host as the compute resource, and click **Next**.
- 10 On the **Review details** page, review the settings, and click **Next**.
- 11 On the **License agreements** page, accept the license agreement, and click **Next**.

- 12 On the **Select storage** page, select the destination storage and optionally the preferred format and the storage policy, and click **Next**.
- 13 On the **Select networks** page, select the port group to which you want the appliance to connect and click **Next**.
- 14 On the **Customize template** page, configure following settings, and click **Next**.

a

Settings	Value
Initial/Current root password	The password of the <i>root</i> user of VMware Photon operating system as per the security compliance policy of your organization or <a href="#">Password Policy</a> . The password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.
Initial/Current <i>shd-admin</i> user password	The password for the <i>shd-admin</i> user account as per the security compliance policy of your organization or <a href="#">Password Policy</a> . The password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character.  <b>Note</b> VMware Skyline Health Diagnostics by default creates a user <i>shd-admin</i> with Administrator Role. This user account must not be deleted and the only account available post deployment. You can use this account to login and create further user accounts.
Host Name	Enter the hostname or FQDN for the appliance (leave blank in case DHCP is desired).
Network IP Address	Enter the IP address for the appliance (leave blank in case DHCP is desired).
Network Prefix	Enter the network prefix for the appliance (leave blank in case DHCP is desired).
Default IPv4 Gateway	Enter the default gateway for the appliance (leave blank in case DHCP is desired).
Domain Name Servers	Enter the IP address of the primary and secondary DNS servers, comma or space separated values are accepted (leave blank in case DHCP is desired).
Search Domains	DNS Search Domains [comma (,) or space-separated]. (Leave blank if DHCP is desired)
NTP Servers	Enter the NTP server or servers. Enter comma or space separated values if entering multiple NTP servers. NTP servers can be entered using FQDNs or IP addresses.

- 15 On the **Ready to complete** page, click **Finish**, and wait for the completion of the task.

Task progress will be displayed. The OS boots up with the virtual machine power on and the appliance is ready to use in approximately five minutes.

- 16 Post successful deployment of OVA & plugin registration, the VMware Skyline Health Diagnostics Plugin landing page should change to VMware Skyline Health Diagnostics Plugin home page.

Deployment of the VMware Skyline Health Diagnostics appliance and Registration of the VMware Skyline Health Diagnostics plug-in with the VMware vCenter Server is successful and the client plug-in of the VMware Skyline Health Diagnostics is visible in vSphere Client.

## Registration of Plug-in from VMware Skyline Health Diagnostics User Interface

You can register the VMware Skyline Health Diagnostics with the VMware vCenter Server to perform all the VMware Skyline Health Diagnostics operations from vSphere Client.

As an operator, you want to register single or multiple VMware vSphere Server instances and use the VMware Skyline Health Diagnostics plug-in on vSphere Client as single point for performing diagnostics and reports view.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 VMware vCenter Server version 7.0 and onward.
- 4 You need a valid vSphere, SSO admin credentials.

---

**Caution** The VMware Skyline Health Diagnostics plug-in is only supported for VMware Standalone vCenter Servers.

---

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **vSphere Plugin Registration**.  
The vSphere plug-in management page will be loaded.
- 4 Click the **+** icon, to open a register vSphere plugin wizard.  
Register vSphere plug-in dialog box will be displayed.
- 5 Enter the VMware vCenter Server FQDN or IP address in the **Target**.
- 6 Enter the VMware vCenter Server appliance SSO admin user credentials.
- 7 Click **Submit**.
  - It authenticates the entered SSO credentials with the VMware vCenter Server appliance.

- Registers the VMware Skyline Health Diagnostics plug-in to the entered target VMware vCenter Server.
  - Wizard closes with success message **SHD Extension registered on vCenter Server: xx.xx.xx.xx** after successful registration of the VMware Skyline Health Diagnostics plug-in.
  - If the VMware Skyline Health Diagnostics plug-in registration process with the target VMware vCenter Server fails, then the **Register vSphere plug-in** wizard remains open along with corresponding error message visible on top of the wizard.
- 8 To use the VMware Skyline Health Diagnostics plug-in from vSphere Client, log in to vSphere Client Server user interface by entering **SSO administrator** credentials and navigate to **Menu > Skyline Health Diagnostics**

The VMware Skyline Health Diagnostics plug-in user interface is visible in vSphere Client Server user interface.

## Using the Plug-in from vSphere Client

You can use the VMware Skyline Health Diagnostics user interface from the VMware vSphere Client.

As a vSphere Administrator, you can use the VMware Skyline Health Diagnostics plug-in from vSphere Client to initiate the diagnostics run, run health checks, view the analysis report and manage the configurations.

### Prerequisites

- 1 The VMware Skyline Health Diagnostics plug-in must be registered with the VMware vCenter Server instance.
- 2 You need a valid VMware vCenter Server SSO admin user credentials.

### Procedure

- 1 Log in to the VMware vCenter Server user interface using SSO admin user credentials.
- 2 From the top menu, click **Menu > Skyline Health Diagnostics** .  
The welcome page of Skyline Health Diagnostics plug-in is loaded into VMware vCenter Server user interface.
- 3 Click **Start Analyze** . You should be redirected to the **Tasks** tab.
- 4 Select **New Diagnostics** or **New HealthCheck** and choose checks from the displayed list and click **Next**.
- 5 Click **Connect** from **Target Details** to fetch the VMware vCenter Server inventory view.
- 6 Choose inventory objects on which you want to the run the analysis it could be VMWare vCenter Server or VMWare ESXi hosts from inventory tree view and click **Next**.
- 7 Enter **Tag** , enter **Log Analyze Limit (Days)** under **Additional Details** and click **Next**.

**8 Review Details** and click **Finish**.

A new task would be spawned, click **Refresh Task** to view the status of the analysis task.

**9** After the task is completed, you can view report by clicking on **Show Report**.**10** Select report from checkbox and click on **View** to get the analysis report or click **Download** to save report.**Results**

You will be able to use the VMware Skyline Health Diagnostics plug-in from the VMware vCenter Server user interface to perform the diagnostics on the registered VMware vCenter Server instances and View or Download the analysis reports.

---

**Caution** You must enable and allow the pop up in the browser for the VMware Skyline Health Diagnostics user interface to allow the report download or else it will fail.

---

**Refresh registered VMware vCenter Server**

You can choose to refresh client plug-in of a registered VMware vCenter Server instance from the VMware Skyline Health Diagnostics. After updating configurations on VMware vCenter Server, the VMware Skyline Health Diagnostics plug-in may not work.

As an operator, you can refresh the registered VMware vCenter Server details from the VMware Skyline Health Diagnostics, if the VMware Skyline Health Diagnostics plug-in stops working post updating any critical information on VMware vCenter server.

**Prerequisites**

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 VMware Skyline Health Diagnostics must be registered with VMware vCenter Server instance.
- 4 You need to have valid VMware vCenter Server, SSO admin credentials.

**Procedure**

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **vSphere Plugin Registration**.  
vSphere plug-in Management will be loaded.
- 4 Select the VMware vCenter server and Click on the **Refresh** icon, it should open the wizard.
- 5 Enter the VMware vCenter Server appliance new SSO admin user credentials.

## 6 Click **Refresh**.

- It authenticates the entered VMware vCenter Server SSO credentials by performing a login to the VMware vCenter Server and refreshes VMware Skyline Health Diagnostics plug-in on the VMware vCenter client.
- Once the plug-in refresh is successful the pop-up will close, and you will see the **SHD Extension registered on vCenter Server: xx.xx.xx.xx** message.
- If the error is observed while the registration of the VMware vCenter Server, the **Refresh vSphere plug-in** pop will not close, and corresponding error message is displayed on its top.

## 7 To use the VMware Skyline Health Diagnostics plug-in from vSphere Client, log in to vSphere Client user interface with **SSO Administrator** credentials and Navigate to **Menu > Skyline Health Diagnostics**.

### Results

Refresh of vSphere with the VMware Skyline Health Diagnostics is successful, and the client plug-in of VMware Skyline Health Diagnostics will be visible and working into vSphere Client.

## Deregistration of Plug-in from VMware Skyline Health Diagnostics User Interface

You can remove a registered vSphere instance from the VMware Skyline Health Diagnostics, this will also remove the VMware Skyline Health Diagnostics client plug-in from the VMware vCenter Server.

If the VMware Skyline Health Diagnostics plug-in stops working or you no longer want to use the VMware Skyline Health Diagnostics client plug-in in the VMware vCenter Server, you can remove the registered VMware vCenter Server from the VMware Skyline Health Diagnostics.

### Prerequisites

- 1 Verify that you can access the VMware Skyline Health Diagnostics user interface.
- 2 Verify that you have the administrator privileged user credentials to log in the VMware Skyline Health Diagnostics.
- 3 VMware Skyline Health Diagnostics must be registered with VMware vCenter Server instance.
- 4 You need to have valid VMware vCenter Server, SSO admin credentials.

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **vSphere Plugin Registration**.  
vSphere plug-in Management will be loaded.

- 4 Select the VMware vCenter server and Click on the **Delete** icon, it should open the wizard.
- 5 Enter the VMware vCenter Server appliance SSO admin user credentials.
- 6 Click **Delete**.
  - It authenticates the entered VMware vCenter Server credentials by performing log in to the target VMware vCenter Server and deletes the VMware Skyline Health Diagnostics plug-in from the VMware vCenter HTML client.
  - If the deletion of plug-in is successful, the pop-up closes, and you see the **SHD Extension removed on vCenter Server: xx.xx.xx.xx** message.
  - If the error is observed while the removal of VMware Skyline Health Diagnostics plug-in from the VMware vCenter Server, the **Delete vSphere Plug-in** pop will not close, and corresponding error message is displayed on its top.

### Results

The VMware Skyline Health Diagnostics plug-in is successfully unregistered from the VMware vCenter Server, and the VMware Skyline Health Diagnostics plug-in will not be visible in the VMware vCenter Server user interface.

## Help and Support

You can get help on issues faced during installation, operations, or any queries on the VMware Skyline Health Diagnostics.

You can download the support bundle for the VMware Skyline Health Diagnostics, you might want to share with the VMware support.

### Prerequisites

- Verify that you can open the user interface of the VMware Skyline Health Diagnostics in the browser window.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

---

**Caution** You must enable and allow the pop up in the browser for the VMware Skyline Health Diagnostics user interface to allow the support bundle download or else it will fail.

---

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Help and Support**.
- 4 Click **Support Bundle**.

- 5 In the absence of user interface, open the Skyline Health Diagnostics appliance console using the VMware vSphere client or Secure Shell (SSH) client.
- 6 Log in as **root** user.
- 7 To collect the log bundle run the command **shd-support** on the shell. This command collects the log bundle in the current folder.
- 8 Download the log bundle to your system using **winSCP** or **SCP**.
- 9 For any install issue, take the screenshot and collect the details from console.
- 10 Send an email to **shd-support@vmware.com** with issue details, screenshots along with log bundle attached.

### Results

VMware starts looking into the issue and will reach out to you.

## View the CEIP Data Collected for Reporting and Analytics

The administrators or the security teams in your organization might be interested to know the data collected by the VMware Skyline Health Diagnostics as part of CEIP. The **Tool Usage Report** provides insight into the data collected.

### Prerequisites

- Verify that you can open the user interface of the VMware Skyline Health Diagnostics in the browser window.
- Verify that you have either *SHD Operator* or *SHD Administrator* privileged user credentials to log in the VMware Skyline Health Diagnostics.

---

**Caution** You must enable and allow the pop up in the browser for the VMware Skyline Health Diagnostics user interface to allow the reports download or else it will fail.

---

### Procedure

- 1 Log in to the VMware Skyline Health Diagnostics user interface on a supported web browser using a user with administrator privilege.
- 2 Click on the **Settings** tab from the top-menu.
- 3 In the left pane, select **Help and Support**.
- 4 Click **Tool Usage Report**.
- 5 The download of the report should start.
- 6 Once download complete, open the report to see the data collected by the VMware Skyline Health Diagnostics, that you will be sharing with VMware.



## Results

The report having the details about the data collected by the VMware Skyline Health Diagnostics.

# Scale Limits for VMware Skyline Health Diagnostics

# 4

This section defines the scale and max configurable limits supported by the VMware Skyline Health Diagnostics to function effectively considering the default resource allocation of the VMware Skyline Health Diagnostics appliance.

Read the following topics next:

- [Scale Limits](#)

## Scale Limits

This section provides the maximum supported limits for the analyze operation on the VMware Skyline Health Diagnostics.

### Maximum Limits for the Analyze Operation

- 1 The maximum number of ESXi hosts allowed to select during the analyze operations are *sixty-four*. You can select the VMware vCenter Server along with VMware ESXi host limit.
- 2 The maximum number of parallel analysis runs allowed are *four*, across the VMware Skyline Health Diagnostics. This means if five users want to run the analysis in parallel, only four will be executed and other analyze operations will error out. After an analyze operation is completed, the user can start the new analysis operation.
- 3 You can submit four parallel analyze operations with maximum *sixty-four* VMware ESXi hosts in each request.

### Maximum Limits for all the Activities

<b>Maximum Upgrade Summary</b>	Last five upgrade activities will be displayed.
<b>Download History Summary</b>	Last five download activities will be displayed.
<b>Maximum Tasks displayed</b>	Recent <b>Task</b> view displays ten most recent tasks.

Maximum number of hosts  
allowed to select in  
the analysis operation

You can select maximum *sixty-four* VMware ESXi hosts for and one VMware vCenter Server in an analyze operation run.

Maximum number of  
parallel runs across  
SHD

The maximum number of parallel analyses run allowed are *four* across the Skyline Health Diagnostics.

# Ports and Protocols

## 5

The VMware Skyline Health Diagnostics provides user interface over the network. If the internet connectivity is available, it can download the software updates and perform VCG database updates using the user interface. It also communicates to VMware CEIP Service if CEIP is opted in.

The VMware Skyline Health Diagnostics Server interacts with VMware Services hosted in the VMware environment, outside of the customer on-premises infrastructure to download updates, and signatures, and share the CEIP data. The VMware Skyline Health Diagnostics Server also communicates with products and solutions in the on-premises environment being analyzed to collect logs, configuration information etc. Protocols of these communication may vary depending on the Product, types of checks etc.

The VMware Skyline Health Diagnostics requires following protocols and ports for inbound & outbound connections.

### Inbound Interaction

The VMware Skyline Health Diagnostics client can interact with VMware Skyline Health Diagnostics Server on the secure port, using the secure protocol.

Purpose	Destination URL	Protocol	Destination Port	Type of Interaction
Web user interface	https://<IP or FQDN of the VMware Skyline Health Diagnostics appliance>/Panalyze	HTTPS	443	Inbound
Connect to the VMware Skyline Health Diagnostics appliance console over the SSH	ssh_remote_username@remote_host	SSH	22	Inbound

### Outbound Interaction

VMware Skyline Health Diagnostics requires following outbound Interaction to receive or send the data to successfully perform its tasks.

Purpose	Destination URL	Protocol	Destination Port	Type of Interaction
Download new patches, updates	<a href="https://shd-download.vmware.com">https://shd-download.vmware.com</a>	HTTPS	443	Outbound
Download the VMware Compatibility Guide updates	<a href="https://shd-download.vmware.com">https://shd-download.vmware.com</a>	HTTPS	443	Outbound
Customer Experience Improvement Program	<a href="https://vcsa.vmware.com">https://vcsa.vmware.com</a>	HTTPS	443	Outbound

# Supported Versions and Compatibilities

## 6

This section provides the supported versions and interoperability of Skyline Health Diagnostics.

VMware supports the VMware Skyline Health Diagnostics 4.0.0 (latest) and 3.5.2 (latest - 1) versions. To raise a support request or to get a fix for an issue, your VMware Skyline Health Diagnostics must be on one of these versions. If you do not have any of these latest versions, upgrade to the latest version as soon as possible.

**Table 6-1. Support VMware Product Matrix**

Product Name	Supported Product Versions
VMware vCenter Server	6.5, 6.7, 7.0 and 8.0*.
VMware ESXi	6.5, 6.7, 7.0 and 8.0*.
VMware vSAN	6.5, 6.7, 7.0 and 8.0*.
VMware Cloud Foundation	4.0, 4.1, 4.2, 4.3, 4.4, 4.5 and 5.0** Upgrade Assessment*** feature is supported for VMware Cloud Foundation version 4.5 and 5.0.
VMware Horizon***	7.0 and 8.0.
VMware SD-WAN***	3.4, 4.0, 4.2, 4.3, 4.5, 5.0, 5.1 and 5.2.
VMware vCenter Cloud Gateway	8.x.

**Note** \* Versions of this product are only supported from the VMware Skyline Health Diagnostics 3.5.2 version and above.

\*\* Versions of this product are only supported from the VMware Skyline Health Diagnostics 4.0.0 version and above.

\*\*\* The products or features are only supported from the VMware Skyline Health Diagnostics 4.0.0. version and above.