

VMware Skyline Collector User Guide

VMware Skyline Collector 2.5

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

Copyright © 2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	About VMware Skyline Collector User Guide	4
2	Network Requirements	5
3	Access the Skyline Collector	6
4	System Status	7
	Manage Collector	7
	Restart Skyline Collector	8
	Stop Skyline Collector	8
	DeRegister Skyline Collector	9
	Products Added	10
5	Configuration	12
	vCenter Server	13
	NSX-V (NSX Data Center for vSphere)	16
	NSX-T (NSX-T Data Center)	17
	Horizon View	19
	vRealize Operations	20
	Network Configuration	22
	Auto-Upgrade	23
	Collector Name	24
	Active Directory Authentication	24
	Web Server Certificate	25
	Root Password Expiration	26
6	Change the admin Account Password	27
7	Update Skyline Collector	28
8	Customer Experience Improvement Program (CEIP)	29

About VMware Skyline Collector User Guide

1

The VMware Skyline Collector User Guide provides instructions for the VMware® Skyline™ Collector. The guide contains information about managing the Skyline Collector, adding, editing, or removing products, and information regarding the privacy and security of data that VMware receives.

Intended Audience

This information is intended for anyone who wants to work with the VMware Skyline Collector. It is written for VMware® vSphere® administrators.

Network Requirements

2

The Skyline Collector has the following networking requirements, to ensure proper communication between the Skyline Collector and all products and services.

The Skyline Collector requires network access to VMware products and solutions within your environment, and external network access to VMware.

Table 2-1. External Network Requirements

Connection From	Connection To	Type	Protocol	Port
Skyline Collector	vcsa.vmware.com	HTTPS	TCP/IP	443
Skyline Collector	vapp-updates.vmware.com	HTTPS	TCP/IP	443

Table 2-2. Internal Network Requirements

Connection From	Connection To	Type	Protocol	Port
Skyline Collector	vCenter Server	HTTPS	TCP/IP	443
Skyline Collector	ESXi Hypervisor Hosts	HTTPS	TCP/IP	443
Skyline Collector	5.5 PSC/SSO Provider	HTTPS	TCP/IP	7444
Skyline Collector	6.0 and above PSC/SSO Provider	HTTPS	TCP/IP	443
Skyline Collector	NSX-V Manager	HTTPS	TCP/IP	443
Skyline Collector	NSX-T Manager nodes	HTTPS	TCP/IP	443
Skyline Collector	Horizon Connection Server	HTTPS	TCP/IP	443
Skyline Collector	vRealize Operations Manager	HTTPS	TCP/IP	443
Web Browser	Skyline Collector	HTTPS	TCP/IP	443
Web Browser	Skyline Collector (VAMI)	HTTPS	TCP/IP	5480

Note The tables contain the default port values and might not match a customized environment.

Access the Skyline Collector

3

You must log in to the Skyline Collector to view the status of the Skyline Collector, and to make configuration changes.

Prerequisites

To access the Skyline Collection, you will need the Skyline Collector FQDN or IP address

Procedure

- 1 In a web browser, go to the Skyline Collector, **`https://collector-IP-address-or-FQDN`**.
- 2 Log in as *admin*, or use an Active Directory account if you have enabled Active Directory authentication to the Collector.

The default admin password is *default*. You are required to change the *admin* password during the initial configuration of the Collector.

- 3 Click **Log In**.

System Status

4

The **System Status** provides you with an overview of the Skyline Collector health, and management capabilities.

Overview

The **Overview** section displays the health of the Skyline Collector. Additionally, the health of each product added to the Skyline Collector is displayed.

Collector

The [Manage Collector](#) section allows you to Stop, and Restart the Collector, view Collector details, and view the latest log entries for the Skyline Collector.

Endpoints

You can view the products added to the Skyline Collector, including the health of each product endpoint.

This chapter includes the following topics:

- [Manage Collector](#)
- [Products Added](#)

Manage Collector

You can view Skyline Collector details, and Restart or Stop the Collector.

The Manage Collector page displays the following information for the Skyline Collector.

Property	
ID	Alphanumeric unique identifier.
Last Seen	Amount of time since the Skyline Collector sent data to VMware.
Registered Under	The Cloud Services Organization the Skyline Collector is registered with.

You can perform the following actions:

- [Restart Skyline Collector](#)
- [Stop Skyline Collector](#)

The **Collector Log** displays the latest log entries. You can choose to show the latest 200, 400, or 1000 log entries. This information can be used if troubleshooting with VMware Global Support Services (GSS). Click **Show Latest Log** to view the most recent log files for the Skyline Collector.

Restart Skyline Collector

You can restart the Skyline Collector virtual appliance.

Procedure

- 1 In the Skyline Collector, click **System Status**.
- 2 Click **Collector**.
- 3 Click **Restart**.

Results

The Skyline Collector virtual appliance restarts. A restart takes 3 and 5 minutes to complete. The Skyline Collector may not be responsive during this time.

Example: Restart Skyline Collector

Manage Collector

STATUS:

✓ Your Collector is Running

ACTIONS:

RESTARTSTOP

DETAILS:

ID	Last Seen	Registered Under
a few seconds ago		

COLLECTOR LOG:

Number of lines

SHOW LATEST LOG

Stop Skyline Collector

You can stop the Skyline Collector virtual appliance.

Do not stop the Skyline Collector virtual appliance unless troubleshooting with VMware Global Support Services (GSS). Stopping the Skyline Collector will pause the collection of, and sending of product usage data to VMware.

Procedure

- 1 In the Skyline Collector, click **System Status**.
- 2 Click **Collector**.
- 3 Click **Stop**.


Results

If the Skyline Collector is in a Stopped state, an alert appears within the Skyline Collector stating **Your Collector is Not Running**. Stopping the Skyline Collector does not shut down the virtual appliance. The virtual appliance remains running and the Skyline Collector remains available.

Example: Stop Collector

Manage Collector

STATUS:

 Your Collector is Running

ACTIONS:

RESTART
STOP

DETAILS:

ID	Last Seen	Registered Under
a few seconds ago		

COLLECTOR LOG:

Number of lines 200

SHOW LATEST LOG

What to do next

Click **Start** to restart the Skyline Collector.

DeRegister Skyline Collector

Remove an Inactive Skyline Collector from Skyline.

The capability to remove an inactive Skyline Collector is available within Skyline Advisor. Follow these steps to remove an inactive Skyline Collector from your Cloud Services Organization.

A Skyline Collector becomes Inactive if it has not communicated with VMware after 60 minutes. If your Skyline Collector is in a Healthy state, power-off the Skyline Collector virtual appliance, wait ~60 minutes, then view the status of the Skyline Collector within Skyline Advisor.

Prerequisites

If a Skyline Collector was removed from your environment without deregistering it first, you can remove the Skyline Collector from your account using the DeRegister function within Skyline Advisor.

Important Only users assigned the Skyline Administrator service role can DeRegister an inactive Skyline Collector. Users assigned the Skyline User service role do not have this capability. For more information regarding Skyline Advisor service roles, see [Service Roles in Skyline Advisor](#).

Procedure

- 1 In a web browser, go to <https://skyline.vmware.com/advisor>. Login to Cloud Services.
You can use your existing My VMware account details to log in to VMware Cloud Services. You do not need to create a new account for the purposes of utilizing VMware Cloud Services.
- 2 Within Skyline Advisor, click **Dashboard**.
- 3 Click **Show Collector Details**.
- 4 Find the Skyline Collector in an Inactive state that you want to DeRegister from Skyline. Click **DeRegister**.
- 5 Click **Yes** to confirm that you want to DeRegister the Skyline Collector from Skyline.

Results

The Skyline Collector does not appear within the Collector Details page within Skyline Advisor.

Products Added

You can view the products added to the Skyline Collector, including the health of each product endpoint.

Each product added to the Skyline Collector is listed under the product name. The product names include vCenter Server, NSX-V, NSX-T, Horizon View, and vRealize Operations.

For each product, expand the object name. Each product endpoint is displayed.

The following table lists all endpoints for each product.

Product	Endpoint
vCenter Server	VC_EXTRA
	VC_HOSTS
	VC_CHANGES
NSX-V (NSX Data Center for vSphere)	NSX
NSX-T (NSX-T Data Center)	NSX_T

Product	Endpoint
Horizon View	HORIZON_VIEW
vRealize Operations	VROPS

For each product endpoint, the only action that can be performed is **Restart**. Restarting the product endpoint stops, then restarts the data collection for that particular product endpoint.

The following details are available for each product endpoint:

Property	Details
Host	Product object name.
Type	The product endpoint type.
Last Seen	The amount of time since this product endpoint collected data.
User Account	The user account used to add the product to the Skyline Collector.

The following is available for the last known execution details.

Property	Details
Message	Details regarding whether the data collection was successful, or if there was an error.
State	Whether the data upload was successful, or not
Payload File	The filename uploaded to VMware.
Payload Size	The size of the file uploaded to VMware.
Last execution	The amount of time since the last file was uploaded to VMware.

The **Collector Log** displays the latest log entries. You can choose to show the latest 200 log, 400 log, or 1000 log entries. This information can be used if the troubleshooting with VMware Global Support Services (GSS). Click **Show Latest Log** to view the most recent log files for the Skyline Collector.

Configuration

5

You can configure the Skyline Collector, including products, network configuration, and Active Directory authentication.

The following options are available within the **Configuration** page of the Skyline Collector.

- vCenter Server
- NSX-V (NSX Data Center for vSphere)
- NSX-T (NSX-T Data Center)
- Horizon View
- vRealize Operations
- Network Configuration
- Auto Upgrade
- Collector Name
- Active Directory Authentication
- Web Server Certificate
- Root Password Expiration

This chapter includes the following topics:

- [vCenter Server](#)
- [NSX-V \(NSX Data Center for vSphere\)](#)
- [NSX-T \(NSX-T Data Center\)](#)
- [Horizon View](#)
- [vRealize Operations](#)
- [Network Configuration](#)
- [Auto-Upgrade](#)
- [Collector Name](#)
- [Active Directory Authentication](#)
- [Web Server Certificate](#)

- [Root Password Expiration](#)

vCenter Server

Configure product usage data collection for vSphere in the Skyline Collector.

Prerequisites

The following role/privileges are required for the account used to add the vCenter Server to the Skyline Collector. These role/privileges are sufficient for both collecting product usage data, and transferring support bundles with Skyline Log Assist.

- vCenter Server Read-Only role
- Global.Diagnostics
- Global.Health
- Global.Licenses
- Global.Settings
- Host profile.View

For detailed instructions for how to create a user account with the given permissions, see [Knowledge Base Article 59661](#).

Important You must assign the required role/privileges to a user account. Assigning the required role/privileges to a group, and using a user account within that group to vCenter Server to the Skyline Collector fails the privileges check within the Skyline Advisor.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **PRODUCTS**, click **vCenter Server**.

3 Choose one of the following three options:

Option	Description
Add vCenter Server	To add a new vCenter Server to the Skyline Collector, click Add vCenter Server . To complete the adding of a vCenter Server to the Skyline Collector, follow the given steps.
Edit vCenter Server	<p>To edit a vCenter Server, click Edit.</p> <p>You can only edit the following properties for a vCenter Server instance:</p> <ul style="list-style-type: none"> ■ Account Username ■ Account Password ■ PSC/SSO Host Address ■ Collector From All Datacenters <p>After you have finished editing the vCenter Server instance, click Update.</p>
Delete vCenter Server	<p>To delete a vCenter Server from the Skyline Collector, click Delete.</p> <p>Deleting a vCenter Server removes it from the Skyline Collector, and disables the collection of product usage data for all vCenter Server objects. Findings, Upgrade Recommendations, and Log Assist will not be available for the deleted vCenter Server (vSphere) environment.</p>

4 After clicking **Add vCenter Server**, follow these steps to add a vCenter Server to the Skyline Collector.

- a Enter the **FQDN/IP Address** of the vCenter Server.
- b Enter a **Account Username** for connecting to the vCenter Server, from the Skyline Collector. This account must have the minimum required privileges, as detailed within the Prerequisites.
- c Enter the **Account Password**.

- 5 If you are using an external PSC/SSO, or are using a custom Single-Sign-On domain, toggle the **Use Custom SSO Configuration** button to the right. The switch states **Yes**, and turns





Green [].

- a Enter the **PSC/SSO Host Address**.
- b If you did not change the PSC/SSO configuration from the default, you DO NOT have to complete the Advanced Options (Optional) fields. If you are using a custom SSO domain, enter the **SSO Admin URL**, **SSO STS URL**, and **Lookup Service URL** for the custom SSO domain.

To locate your SSO domain Advanced Options, see the vCenter Server vpxd.cfg file.

- In vCenter Server Appliance 6.x, the vpxd.cfg file is at /etc/vmware-vpx/.
- In Windows Server, the vpxd.cfg file is at C:\ProgramData\VMware\VMware VirtualCenter\vpdx.cfg.
- In vCenter Server 6.0, the vpxd.cfg file is at C:\ProgramData\VMware\vCenterServer\cfg\vmware-vpx.

- 6 You can choose to collect product usage data from all data centers managed by the vCenter Server, or select which data centers to include in the collection of product usage data. A Datacenter consists of the ESXi hosts, virtual machines, and the configuration, feature usage, and perform data for these objects.

Option	Description
Yes, Collect from All data centers	To Collect from All data centers, toggle the switch to the right. The switch  states Yes , and turns Green []. The Skyline Collector collects product usage data from all data centers managed by the vCenter Server.
No, only Collect from select data centers	To only Collect from select data centers, toggle the switch to the left. The switch  states No , and turns Grey []. Click Add . A list of data centers is displayed. Check the checkbox next to each Datacenter that you want to include in Skyline.

- 7 To complete adding the vCenter Server to the Skyline Collector, click **Add**.

Results

This vSphere environment is analyzed for potential issues, security vulnerabilities, impacts to usability, and configuration recommendations. The results of this analysis appear in Skyline Advisor. To add additional vCenter Servers to the Skyline Collector, repeat this process.

Note Disabling product use data collection from select data centers may prohibit VMware from providing an optimal support experience.

NSX-V (NSX Data Center for vSphere)

Configure the product usage data collection for NSX-V (NSX Data Center for vSphere) in the Skyline Collector.

Prerequisites

For NSX-V version 6.4.5 and below, the NSX Auditor role does not have sufficient privileges to generate and collect support bundles from NSX-V objects. To generate and collect support bundles from NSX-V objects, a user account with the NSX Administrator role is required. Therefore, you have two options for adding NSX-V version 6.4.5 to a Skyline Collector.

For the collection of product usage data only:

- NSX Auditor

Important If an account with the NSX Auditor role is used to add NSX-V, the following is displayed within Skyline Advisor:

- On the Collector Details page, the Status of NSX-V is: Insufficient Privileges.
- On the Initiate Log Transfer page, the Privileges check for NSX-V, and all NSX-V components fail.

If using an account with the NSX Auditor role, you cannot transfer support bundles to VMware GSS using Skyline Log Assist.

For the collection of both product usage data, and transferring support bundles with Log Assist:

- NSX Administrator

For NSX-V version 6.4.6, and above:

The NSX Auditor role in NSX-V version 6.4.6 supports the ability to transfer NSX Edge support bundles. This capability was not available in NSX-V versions previous to 6.4.6. Therefore, a user account assigned the NSX Auditor role can be used for product usage data collection, and for the transferring of support bundles using Log Assist.

For the collection of both product usage data, and transferring support bundles with Log Assist:

- NSX Administrator

Important You must assign the required role/privileges to a user account. Assigning the required role/privileges to a group, and using a user account within that group to add NSX-V to the Skyline Collector fails the privileges check within the Skyline Advisor.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **PRODUCTS**, click **NSX-V**.

3 Choose one of the following three options:

Option	Description
Add NSX-V	To add a new NSX Manager to the Skyline Collector, click Add NSX-V . Follow the given steps to add NSX-V to the Skyline Collector.
Edit NSX-V	To edit NSX-V, click Edit . You can only edit the following properties for NSX-V: <ul style="list-style-type: none"> ■ Account Username ■ Account Password After you have finished editing NSX-V, click Update .
Delete NSX-V	To delete NSX-V from the Skyline Collector, click Delete . Deleting NSX-V removes it from the Skyline Collector, and disables the collection of product usage data for all NSX-V objects. Findings, Upgrade Recommendations, and Log Assist will not be available for the deleted NSX-V environment.

4 After clicking **Add NSX Manager**, follow these steps to add an NSX Manager to the Skyline Collector.

- Enter the **FQDN/IP Address** of the NSX Manager.
- Enter a **Account Username** for connecting to the NSX-V. This account must have the minimum required privileges, as detailed within the Prerequisites.
- Enter the **Account Password**.

5 To complete adding NSX-V to the Skyline Collector, click **Add**.

This NSX-V environment is analyzed for potential issues, security vulnerabilities, impacts to usability, and configuration recommendations. The results of this analysis appear in Skyline Advisor. Repeat this process to add additional NSX-V instances to the Skyline Collector.

NSX-T (NSX-T Data Center)

Configure the product usage data collection for NSX-T (NSX-T Data Center) in the Skyline Collector.

Prerequisites

For NSX-T, the NSX Auditor role does not have sufficient privileges to generate and collect support bundles from NSX-T objects. To generate and collect support bundles from NSX-T objects, a user account with the NSX Administrator role is required. Therefore, you have two options for adding NSX-T to a Skyline Collector.

For the collection of product usage data only:

- NSX Auditor

Important If an account with the NSX Auditor role is used to add NSX-T, the following is displayed within Skyline Advisor:

- On the Collector Details page, the Status of NSX-T is: Insufficient Privileges.
- On the Initiate Log Transfer page, the Privileges check for NSX-T, and all NSX-T components fail.

If using an account with the NSX Auditor role, you cannot transfer support bundles to VMware GSS using Skyline Log Assist.

For the collection of both product usage data, and transferring support bundles with Log Assist:

- NSX Enterprise Administrator

Important You must assign the required role/privileges to a user account. Assigning the required role/privileges to a group, and using a user account within that group to add NSX-T to the Skyline Collector fails the privileges check within the Skyline Advisor.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **PRODUCTS**, click **NSX-T**.
- 3 Choose one of the following three options:

Option	Description
Add NSX-T	To add NSX-T to the Skyline Collector, click Add NSX-T . To add NSX-T to the Skyline Collector, follow the given steps.
Edit NSX-T	To edit NSX-T, click Edit . You can only edit the following properties for NSX-T: <ul style="list-style-type: none"> ■ Account Username ■ Account Password After you have finished editing NSX-T, click Update .
Delete NSX-T	To delete NSX-T from the Skyline Collector, click Delete . Deleting NSX-T removes it from the Skyline Collector, and disables the collection of product usage data for all NSX-T objects. Findings, Upgrade Recommendations, and Log Assist will not be available for the deleted NSX-T environment.

- 4 After clicking **Add NSX-T**, follow these steps to add an NSX-T to the Skyline Collector.
 - a Enter the **FQDN/IP Address** of the NSX-T Manager nodes cluster virtual IP address (VIP). See [Configure a Virtual IP Address for a Cluster](#) (NSX-T Data Center documentation) for more details.
 - b Enter a **Account Username** for connecting to NSX-T. This account must have the minimum required privileges, as detailed within the Prerequisites.
 - c Enter the **Account Password**.
- 5 To complete adding NSX-T to the Skyline Collector, click **Add**.

Results

This NSX-T environment is analyzed for potential issues, security vulnerabilities, impacts to usability, and configuration recommendations. The results of this analysis appear in Skyline Advisor. To add additional NSX-T environments to the Skyline Collector, repeat this process.

Horizon View

Configure product usage data collection for Horizon View in the Skyline Collector.

Prerequisites

The following role/privileges are required for the account used to add the Horizon Connection Server to the Skyline Collector. These role/privileges are sufficient for both collecting product usage data, and transferring support bundles with Log Assist.

- Administrator (read-only) Role
- Collect Operation Logs

Important If you are using Skyline Collector version 2.3, or below, you must create a new role for Horizon View with the Collect Operations Logs privilege. The role must be named **LogCollector**.

For Skyline Collector version 2.4 and above, there is no requirement to name the role **LogCollector**.

Important You must assign the required role/privileges to a user account. Assigning the required role/privileges to a group, and using a user account within that group to add Horizon View /to the Skyline Collector will fail privileges check within Skyline Advisor.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **PRODUCTS**, click **Horizon View**.

3 Choose one of the following three options:

Option	Description
Add Horizon View	To add a new Horizon Connection Server to the Skyline Collector, click Add Horizon View . Follow the given steps to add a Horizon Connection Server to the Skyline Collector.
Edit Horizon View	To edit a Horizon Connection Server, click Edit . You can only edit the following properties for a Horizon Connection Server: <ul style="list-style-type: none"> ■ Account Username ■ Account Password After you have finished editing the Horizon Connection Server, click Update .
Delete Horizon View	To delete a Horizon Connection Server from the Skyline Collector, click Delete . Deleting a Horizon Connection Server removes the Horizon Connection Server from the Skyline Collector, and disables the collection of product usage data for that Horizon Connection Server. Findings, Upgrade Recommendations, and Log Assist will not be available for the Horizon Connection Server.

4 After clicking **Add Horizon View**, follow these steps to add a Horizon Connection Server to the Skyline Collector.

- Enter the **FQDN/IP Address** of the Horizon Connection Server.
- Enter a **Account Username** for connecting to the Horizon Connection Server, from the Skyline Collector. This account must have the minimum required privileges, as detailed within the Prerequisites.
- Enter the **Account Password**.

5 To complete adding the Horizon Connection Server to the Skyline Collector, click **Add**.

Results

This Horizon View environment is analyzed for potential issues, security vulnerabilities, impacts to usability, and configuration recommendations. The results of this analysis appear in Skyline Advisor. Repeat this process to add additional Horizon Connection Servers to the Skyline Collector.

vRealize Operations

Configure the product usage data collection for vRealize Operations in the Skyline Collector.

Prerequisites

Important Skyline Log Assist does not support the transferring of support bundles to VMware GSS. Any vRealize Operations Manager instances added to a Skyline Collector will not appear within the Log Assist page of Skyline Advisor.

The following role/privileges are required for the account used to add the vRealize Operations Manager to the Skyline Collector. These role/privileges are sufficient for collecting product usage data.

- vRealize Operations Read-Only Role

Important You must assign the required role/privileges to the user account. Assigning the required role/privileges to a group, and using a user account within that group to add vRealize Operations Manager to the Skyline Collector fails the privileges check within Skyline Advisor.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **PRODUCTS**, click **vRealize Operations**.
- 3 Choose one of the following three options:

Option	Description
Add vRealize Operations	To add a new vRealize Operations Manager to the Skyline Collector, click Add vRealize Operations . To add a vRealize Operations Manager to the Skyline Collector, follow the given steps.
Edit vRealize Operations	To edit a vRealize Operations Manager, click Edit . You can only edit the following properties for vRealize Operations Manager: <ul style="list-style-type: none"> ■ Account Username ■ Account Password After you have finished editing vRealize Operations Manager, click Update .
Delete vRealize Operations	To delete a vRealize Operations Manager from the Skyline Collector, click Delete . Deleting a vRealize Operations Manager removes the vRealize Operations Manager from the Skyline Collector, and disables the collection of product usage data for that vRealize Operations Manager. Findings, and Upgrade Recommendations is not available for the vRealize Operations Manager.

- 4 After clicking **Add vRealize Operations**, follow these steps to add a vRealize Operations Manager to the Skyline Collector.
 - a Enter the **FQDN/IP Address** of the vRealize Operations Manager.
 - b Enter a **Account Username** for connecting to the vRealize Operations Manager, from the Skyline Collector. This account must have the minimum required privileges, as detailed within the Prerequisites.

If using an Active Directory account, enter the username only. You do not need to provide the domain name.

Example, for the user admin@corp.local, enter '**admin**' only.

- c Enter the **Account Password**.
- d To use a domain user account for adding the vRealize Operations Manager to the Skyline Collector, enter the Authentication Source name. This is the domain name.

For the Domain CORP.LOCAL, enter **CORP** within the Authentication Source text field.

- 5 To complete adding the vRealize Operations Manager to the Skyline Collector, click **Add**.

Results

This vRealize Operations Manager is analyzed for potential issues, security vulnerabilities, impacts to usability, and configuration recommendations. The results of this analysis appear in Skyline Advisor. To add additional vRealize Operations Managers to the Skyline Collector, repeat this process.

Network Configuration

Configure hostname verification, and configure a proxy, for the Skyline Collector communication to VMware.

Hostname Verification verifies that the Skyline Collector is connecting to VMware (vcsa.vmware.com), by looking at the 'dnsName' and 'subjectAltName'. Hostname Verification ensures customer product usage data is being sent to VMware.

Also, the Skyline Collector supports a proxy for accessing the Internet.



Prerequisites

Ensure the Skyline Collector can communicate with the following external network destinations:



- vcsa.vmware.com
- vapp-updates.vmware.com

Procedure


- 1 Click **Configuration** in the Skyline Collector user interface.
- 2 Under **COLLECTOR**, click **Network Configuration**.
- 3 Follow these steps to Enable, or Disable, Hostname Verification.

Option	Description
Enable Hostname Verification	To enable Hostname Verification, toggle the switch to the right. The switch states Enabled , and turns Green [].
Disable Hostname Verification	To disable Hostname Verification, toggle the switch to the left. The switch states Disabled (Not Recommended) , and turns Grey [].

4 To configure a Proxy for the Skyline Collector, follow these steps.

Option	Description
Enable Proxy	To enable a Proxy, toggle the switch to the right. The switch states Enabled , and turns Green []. Follow the given steps to complete the Proxy configuration.
Disable Proxy	To disable a Proxy, toggle the switch to the left. The switch states Disabled , and turns Grey []. No further action is needed.

- a Enter the Proxy **IP Address**.
- b Enter the Proxy **Port Number**.
- c If necessary to authenticate to the Proxy, toggle the Authentication switch to the right.

The switch states **Enabled**, and turns Green [].

The Skyline Collector supports basic access authentication.

The Skyline Collector does not support NTLM access authentication.

- d Enter the Proxy **Username**.
- e Enter the Proxy **Password**.

5 Click **Test & Save**.

Auto-Upgrade

Choose whether to enable the Skyline Collector to automatically upgrade when new versions of the Skyline Collector are available.

When a new version of the Skyline Collector is made available, there are two options for upgrading your Skyline Collector.

1. Manually upgrade your Skyline Collector using the Skyline Collector virtual appliance management interface (VAMI).
2. Automatically upgrade your Skyline Collector by enabling Auto-Upgrade within the Skyline Collector.

If you enable Auto-Upgrade, you no-longer have to complete the manual process of checking for, and upgrading your Skyline Collector.

Prerequisites

The Skyline Collector must be able to communicate with vapp-updates.vmware.com. For more details regarding networking requirements, see the [Skyline Planning and Deployment Guide](#).

Procedure

- 1 In the Skyline Collector, Click **Configuration**.
- 2 Under **COLLECTOR**, click **Auto-Upgrade**.
- 3 To Enable Auto-Upgrade, toggle the switch to the right. The switch states **Yes**, and turns

Green [].

- a Using the **dropdown menu**, pick a day of the week for the Skyline Collector to check for and install updates, if available.
 - b Using the **dropdown menu**, pick a time of the day for the Skyline Collector to check for and install updates, if available.
- 4 To save your settings, click **Set Upgrade Configuration**.

Results

If enabled, your Skyline Collector will check for updates on the day/time that you have chosen. If an update is available, your Skyline Collector will automatically be upgraded.

Collector Name

You can create a friendly name for the Skyline Collector for ease of troubleshooting.

A friendly name describes the environment you are configuring the Skyline Collector to collect data from. This name is used to make it easier for VMware Global Support Services (GSS) to communicate the information about the Skyline Collector with you. An example is: East-Production.

The Collector Name must be between 4 and 32 characters. Letters, numbers, and the following symbols are allowed: period [.] , hyphen [-], and underscore [_].

Procedure

- 1 In the Skyline Collector, Click **Configuration**.
- 2 Under **COLLECTOR**, click **Collector Name**.
- 3 Enter a **Friendly Name** for the Skyline Collector.
- 4 Click **Set Friendly Name**.

Active Directory Authentication

Allow specific Active Directory Users and Groups to access the Skyline Collector.

Enabling Active Directory Authentication within the Skyline Collector allows specific Active Directory Users and Groups to login to the Skyline Collector.

Important To modify the Active Directory configuration, login using the 'admin' account. Active Directory configuration options are disabled when logging-in to the Skyline Collector using an Active Directory User.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **COLLECTOR**, click **Active Directory**.
- 3 Toggle the **Enable Active Directory** switch to **Yes**.
 - a Enter the **Domain Controller Address/IP**.
 - b Enter the **Port** number.
 - c Enter the **Base DN for Users** (optional).
 - d Enter the **Base DN for Groups** (optional).
 - e Enter the **Domain Name**.
- 4 Validate your Active Directory configuration by specifying an Active Directory account Username and Password. These credentials are not stored within the Skyline Collector.
 - a Enter a **Validation Account Username**.
 - b Enter a **Validation Account Password**.
- 5 Add at least one Active Directory User, or Group, that is allowed to log in to the Skyline Collector using their Active Directory Username and Password.
 - a To add a Group, click **Add Group**.
 - b To add a User, click **Add User**.
- 6 Click **Save Configuration**.

Results

Users can now log in to the Skyline Collector using their Active Directory account information.

Web Server Certificate

Replace the Skyline Collector Web Server Certificate used to encrypt the connection between the Skyline Collector web server and the user interface.

The Web Server Certificate is used to encrypt the connection between the Skyline Collector user interface and the local client web-browser.

Procedure

- 1 In the Skyline Collector, click **Configuration**.

- 2 Under **SYSTEM**, click **Web Server Certificate**.
- 3 For Certificate, click **CHOOSE FILE**, then choose the custom certificate file (.cert/.cer/.crt/.pem).
- 4 For Certificate key, click **CHOOSE FILE**, then choose the custom certificate key file (.key/.pem).
- 5 Click **SET CERTIFICATE** to upload the chosen certificates to the Skyline Collector.



Root Password Expiration

You can modify the root password expiration policy.

You can modify the root password expiration policy. This includes enabling or disabling root password expiration and the number of days after which the root password expires.

Procedure

- 1 In the Skyline Collector, click **Configuration**.
- 2 Under **SYSTEM**, click **Root Password Expiration**.
- 3 Follow these steps to Enable, or Disable, Root Password Expiration.

Option	Description
Enable Root Password Expiration	<p>To enable Root Password Expiration, toggle the switch to the right. The switch states Yes, and turns Green [].</p> <p>Choose the number of days after which the Root Password expires. You can choose between 7 and 365 days.</p>
Disable Root Password Expiration	<p>To disable Root Password Expiration, toggle the switch to the left. The switch states Disabled (Not Recommended), and turns Grey [].</p> <p>The Root Password does not expire.</p>

- 4 Click **Save Settings**.

What to do next

If you have set a few days for the root password to expire, enable the Skyline Collector Password Expiry email notification available within Skyline Advisor. Within Skyline Advisor, click **Settings**, to access Email Notification Preferences. See the [Skyline Advisor User Guide](#) for more details.

Change the admin Account Password

6

You can change the Skyline Collector admin user account password at any time.

To change the Skyline Collector admin account password, select the admin account at the top-right corner of the Skyline Collector, and click **Change Password** from the drop-down menu.

The new password must meet the password complexity policy as described on the Change Password page. Click **Set Password** to save the new password.

The 'admin' password must meet the following complexity requirements.

- Minimum length: 8 characters.
- Ensure string has one uppercase letter.
- Ensure string has one special case letter (!@#\$%).
- Ensure string has one digit.
- Ensure string has one lowercase letter.

Update Skyline Collector

7

You can update your Skyline Collector to the latest version using the VMware Appliance Management Interface (VAMI).

Procedure

- 1 In a Web browser, go to the Skyline Collector VAMI, **`https://collector-IP-address-or-FQDN:5480`**.
- 2 Log in as *root*.
- 3 Click **Update**.
- 4 Click **Check Updates**.
- 5 If an update is available, click **Install Updates**.

What to do next

You can enable [Auto-Upgrade](#) within the Skyline Collector to allow the Skyline Collector virtual appliance to automatically check, and upgrade, when a new version of the Skyline Collector is made available. This assists with removing the manual step of updating the Skyline Collector detailed in this topic.

Customer Experience Improvement Program (CEIP)



Participation in the VMware Customer Experience Improvement Program (CEIP) Enhanced participation level is required as part of VMware Skyline.

Joining this program is done as part of the initial configuration of the Skyline Collector.

As part of the Enhanced Customer Experience Improvement Program (CEIP), VMware collects technical information about our customer's use of such products for the purposes given in the following section, such as to improve VMware products and services, and advise our customers on how best to deploy and use our products and services. The data collected through this Customer Experience Improvement Program (CEIP) is separate from the configuration, performance, usage, and consumption data that we collect and use to facilitate delivery of our products and services (such as tracking entitlements, providing infrastructure-related support, monitoring the performance, integrity and stability of the infrastructure, and preventing or addressing service or technical issues) Operational Data).

For additional information regarding the CEIP, see the Trust & Assurance Center at <https://www.vmware.com/solutions/trustvmware/ceip>.

By configuring your VMware products to participate in the Skyline service, each product is enabled to send product usage data to the Skyline services as part of the Customer Experience Improvement Program. You may add, remove, or modify your product configurations at any time. For detailed instructions, see [Knowledge Base \(KB\) article 74676](#).

Participation in the Customer Experience Improvement Program (CEIP) Enhanced participation level can be discontinued for a Skyline Collector at any time by deregistering the Skyline Collector. See [DeRegister Skyline Collector](#) within the [Skyline Advisor User Guide](#) for details.