

VMWARE SKYLINE

Q. What is VMware Skyline™?

A. VMware Skyline™, developed by VMware Global Services, is a proactive support technology available to customers with an active support subscription. Skyline automatically and securely collects, aggregates and analyzes customer-specific product usage data to proactively identify potential issues and improve time-to-resolution.

Q. How does VMware Skyline work?

A. The VMware Skyline Collector is a standalone virtual appliance that automatically and securely collects product usage data. Product usage data includes configuration, feature and performance data. The Collector also listens for changes and events which are streamed to VMware in near real-time.

Analytics are based on a robust rules engine and machine-learning engine. The rules engine is where an ever-growing library of support intelligence, product knowledge and logic are stored to analyze inbound streams of product information.

VMware will use data collected by Skyline to proactively identify potential issues and perform research analysis for service requests to improve the overall stability and reliability of your VMware environment.

Q. How do you manage the VMware Skyline Collector?

A. The VMware Skyline Collector installation and configuration is simple and usually takes no more than 30 minutes to complete. Once complete, ongoing administration is minimal. Data is transferred to VMware over an encrypted channel and stored in secure VMware facilities. Customer data is stored within the Collector for a brief amount of time. VMware analyzes and reports on the information collected as part of your VMware support subscription.

Q. How do I get started?

A. To get started with VMware Skyline, join the [Managed Access Program](#). Customers will be invited in stages to ensure quality and performance for new Skyline customers.

Invitations to participate in Skyline will be sent via email. Within the email invitation are directions for how to download the Skyline Collector virtual appliance along with additional information that will assist you with getting started.

Visit the [VMware Skyline homepage](#) for further information.

Q. How much does Skyline cost?

A. The proactive support capabilities provided by Skyline are available to customers who have an active Production Support or Premier Services contract at no additional cost. Basic Support customers are not eligible to receive proactive support at this time.

Q. Do all support entitlement levels get the same functionality with Skyline?

A. Premier Services customers receive all of Skyline's features and benefits, including expert, consultative recommendations and interactive discussions. Production Support customers will access alerts and recommendations via a self-service portal.

Q. What are Skyline Managed Access Program release stages*?

A. Now: All Premier Services customers in North/South America invited.

Mid-2018: Begin inviting Production Support customers in North/South America.

Mid-2018: Begin inviting EMEA Premier Services customers.

Mid-2018: Begin inviting APJ/ANZ Premier Services customers.

Late 2018/Early 2019: Begin inviting EMEA, APJ/ANZ Production Support customers.

* Release stages and associated timeframes are subject to change.

Q. What product information is being collected today?

A. Today we analyze telemetry information from VMware vSphere® 5.5 and above and NSX® 6.1 and above. With the release of vSAN 6.6, vSAN visibility has also been added. The vSAN™ support capability, associated with VMware Skyline, is called vSAN Support Insight. It provides enhanced visibility into your vSAN environment, allowing Technical Support Engineers (TSEs) to quickly diagnose issues in vSAN environments and reduce time-to-resolution during troubleshooting. Right now, vSAN Support Insight does not require the Skyline Collector, rather is enabled within the release of vSAN 6.6. For more information, visit the vSAN Support Insight page on [Storagehub](#).

In the future, we plan to support all VMware products within Skyline.

Q. Can VMware Skyline be deployed in large VMware environments?

A. VMware recommends an incremental rollout of Skyline in large VMware environments. The Skyline Collector is attached to VMware vCenter Server®(s) and/or NSX Manager™(s) within your environment. You can start with attaching a single vCenter Server to the Skyline Collector. You can attach additional vCenter Servers and/or NSX Managers to the same Skyline Collector incrementally.

If NSX is deployed within your environment, you can attach NSX Manager(s) and NSX Controller™(s) to the Skyline Collector to enable data collection with Skyline.

We recommend one Skyline Collector for every ten VMware product endpoints (vCenter Server, NSX Manager). Also, if you have geographically dispersed environments, we recommend deploying a Skyline Collector at each geographic location. VMware aggregates information collected from multiple Skyline Collectors.

If you have additional questions about VMware Skyline, please talk to your VMware Support Account Manager, Support Account Engineer and/or Technical Account Manager.

Data Privacy and Security Questions

Q. What is the Customer Experience Improvement Program (CEIP)?

A. The Customer Experience Improvement Program (CEIP) provides information that helps VMware to improve our products and services, fix problems and advise you on how best to deploy and use our products. The CEIP policy can be found [here](#). Skyline's policy of data collection falls under the CEIP Enhanced Participation level. Customers must agree to participate in this level of the CEIP during the installation and configuration of the Skyline Collector. The Enhanced Participation level includes all data types under the Standard Participation level plus product logs.

Note: Skyline does not currently collect products logs or support bundles. In the future, Skyline may add product logs and/or support bundles to its data collection.

Q. Where is the data center(s) located where Skyline information is stored?

A. Data is transmitted to secure data centers within the United States, operated by VMware.

Q. What types of Product Usage data are collected?

A. Product Usage data includes the following categories of data:

Configuration data: Technical data about how the customer's organization has configured VMware products and services and related environment information. Examples include version information, product configuration settings and technical data relating to the devices accessing those products and services.

Performance data: Data about the performance of VMware products and services. Examples include metrics of the performance and scale of VMware products and services, response times for user interfaces and details about API calls.

Note: Product log data is not collected today. Product log data may be included in Skyline data collection in the future. Production log collection authorization is included within the CEIP Enhanced Participation level that you agree to at the time of Skyline configuration. Product logs are generated by VMware products during deployment of the product. Product logs record system state and events during product operations, in a semi-structured or unstructured form.

Skyline data collection may include customer identifiable information in the form of ESXi™ hostnames, IP addresses, license keys, customer IDs or entitlement account numbers.

Q. What will Product Usage Data be used for?

A. The use of Product Usage Data is strictly controlled under the CEIP Enhanced Participation level. The Product Analytics Governance Board, comprised of members from Legal, Engineering, Product Security, Sales and IT, defines the program guidelines and regularly monitors execution to help ensure compliance within the CEIP policy. Product Usage data is used for the following purposes:

Primarily, customer support: Technical Support Engineers (TSEs) will use configuration data and performance data to identify potential problems within the customers environment. This data will also be used to more quickly resolve problems that have already occurred.

Product deployment analysis: This analysis can only be used by your account representative to discuss how best to use relevant products and improve the deployment of said product.

SDDC analysis: Upon deployment, analyze the deployment of VMware SDDC products. Also, VMware Customer Advocacy can survey for new SDDC product releases.

Q. How is customer data protected?

A. Appropriate technical, administrative and organization safeguards are in place to protect the security of customer product usage data. Preventative measures include: encryption in transit, physical security of data centers, appropriate security measures (for backup and disaster recovery) as well as regular recovery solutions or other processing VMware may use to facilitate the auditing process.

Q. Is data encrypted?

A. Data is encrypted during transfer using TLS 1.2 and cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256. Data is not encrypted at rest.

Q. How is the data transferred to VMware?

A. Data is temporarily stored within the Skyline Collector. The Collector transfers the data to VMware over an encrypted channel, using TLS 1.2.

Q. Who owns and manages the data?

A. Since this data is product-specific usage data from VMware software and used primarily for enabling enhanced technical support and product improvement, the data becomes the sole property of VMware.

Q. Who has access to the data?

A. Data is accessible to VMware employees who perform customer support and engagement. Data can be shared across VMware teams to enable cross-product correlation and analysis. VMware employees are required to complete Product Usage Data Training and receive management approval before being able to access the data. Data is not shared with partners or third parties.

Q. How can customers review the data collected?

A. VMware Global Support Services will provide formatted data to the customer within the Operational Summary Report (OSR). The raw data collected will not be provided to the customer.

Q. How long is customer data retained?

A. Customer data is retained for 13 months.

Q. Can Skyline view the workload of my virtual machines?

A. No, Skyline does not look at the details of the workload within the guest Operating System of virtual machines.

Q. Does VMware conduct external infrastructure, network and application penetration tests by an independent and third-party information security provider?

A. Yes.

Q. Does VMware conduct internal infrastructure, network and application penetration tests on a regular basis?

A. Yes.

Q. Will VMware allow an external penetration test or physical onsite audit by a customer nominated third party?

A. No.

Q. Is VMware compliant with any Information Security standards?

A. Not at this time. We are currently investigating ISO 27018, SOC-1, SOC-2 and PCI. Timelines for becoming compliant with any Information Security standards are to be determined.

Q. How are customers notified of security breaches?

A. VMware Security Advisories are posted at [vmware.com/security/advisories](https://www.vmware.com/security/advisories) and sent to subscribers of the VMware Security Advisory mailing list. You can subscribe to this list by following the directions on the "Sign Up for Security Advisories" page at www.vmware.com/security.

Skyline Collector Installation and Security Questions

Q. What are the resource requirements of the Skyline Collector virtual appliance?

A. CPU: 2 vCPU (48MHz active)

Memory: 8GB (409MB active)

Disk Space: 82GB (flat disk, all active and will not grow)

Q. What permissions does the Skyline Collector need to collect product usage data of VMware products?

A. For vCenter Server, read-only permissions are required. The default vCenter Server "read-only" role is sufficient. Also, Global > License is required.

For NSX Manager, Auditor (read-only) permissions are required. Permissions to the NSX Controllers are no longer required with the release of Skyline Collector v1.2.0.

Q. What are the network connectivity requirements for Skyline?

A. Please refer to the VMware Skyline Installation Guide for the network connectivity requirements of the Skyline Collector. The VMware Skyline Installation Guide can be found within the [Skyline Community](#).

Q. How do I install the VMware Skyline Collector?

A. Installing the VMware Skyline Collector is a straightforward process that can be accomplished in a few short steps:

1. Download the Skyline Collector virtual appliance using the link provided to you within your Skyline invitation.
2. Read and accept the VMware Skyline privacy policy statement (CEIP Enhanced Participation level).
3. Register the Skyline Collector using your My VMware account.
4. Connect the Skyline Collector to product endpoints, such as vCenter Server and/or NSX Manager.

Q. Does the Skyline Collector support integration with internal user management systems including Active Directory? Does the Skyline Collector support integration with other IDM solutions?

A. The Skyline Collector version 1.1.1 supports integration with Active Directory. The Skyline Collector does not support any other IDM solutions at this time.

Q. How are user permissions managed on the Skyline Collector?

A. The default administrator account for access the Skyline Collector User Interface is 'admin'.

Q. Does the Skyline Collector support role-based access control?

A. No.

Q. Does the Skyline Collector store user details and/or is sensitive data encrypted?

A. If using Active Directory authentication, usernames are stored within the Skyline Collector. The authentication of a user from the Skyline Collector to the Active Directory authentication server is encrypted. This authentication is private to your environment and is not transmitted to VMware as part of the product usage data collection.

Q. Does the Skyline Collector utilize SSLv3 or TLSv1.1 or lower?

A. No.

Q. Where can I find an overview of the installation?

A. View the Installation and Configuration video [here](#).

Q. Where do I go for more information?

A. See Resources

Resources

- [VMware Skyline homepage](#)
- [Customer Experience Improvement Program](#)
- [Sign up for VMware Skyline Managed Access Program](#)
- [VMware Skyline Community \(VMTN\)](#)

