COHESITY

Version 1.5

September 2024

Cohesity Cluster Secure Phone-Home Channel Security Brief

A Comprehensive Guide to Managing Your Cohesity Cluster Secure Phone-Home Channels

The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services.

ABSTRACT

Cohesity clusters can communicate with remote Cohesity services for telemetry, management, and support. Customers are in full control of their clusters' communication with Cohesity services. This document describes how a cluster can communicate with Cohesity and how customers can identify connection states and enable or disable these communications.

Table of Contents

Introduction to Cohesity Cluster Secure Phone-Home Channels 3
Manage Helios Support Automation and Proactive Wellness Channel 5
View and Control Helios Support Automation and Proactive Wellness Channel Status…… 6
Use Helios Global Active Management Channel 7
View and Control Helios Global Active Management 8
Manage Product Usage Statistics Channel 11
View and Control Product Usage Statistics Channel 11
Enable Support Channel for Remote Troubleshooting 13
View and Control Support Channel 14
Your Feedback 18
About the Authors 18
Document Version History 18

Figures

Figure 1: Cohesity Cluster Secure Phone-Home Communication Channels 3
Figure 2: Support Channel Access Protected by Token Exchange (Cohesity 6.5.1b and above) 14
Figure 3: Support Channel Access Protected by Token Exchange (Cohesity 6.8.1 and above) 14

Introduction to Cohesity Cluster Secure Phone-Home Channels

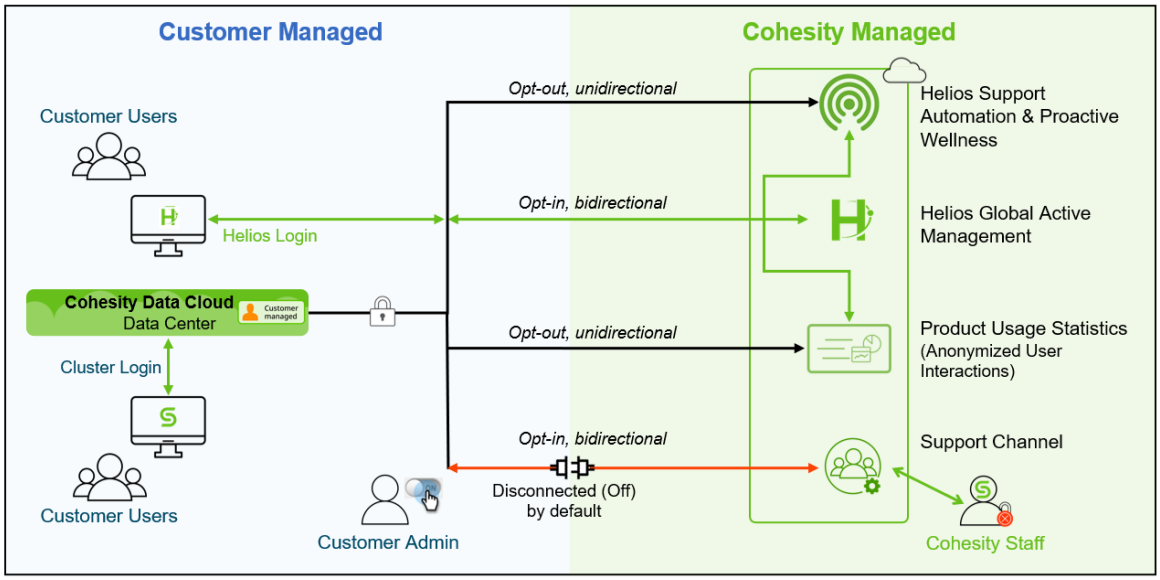
Cohesity clusters have four secure Phone-home channels with Cohesity services. When you set up a Cohesity cluster, you can configure which Cohesity services the cluster communicates with as much or as little as your business needs dictate.

- **Helios Support Automation & Proactive Wellness** (*Opt-out*). Cohesity's support mechanism that detects potential problems and proactively alerts cluster administrators for remediation.
- **Helios Global Active Management** (*Opt-in*). Global active management and monitoring for your Cohesity clusters with predictive analytics using machine learning. Includes protection from, detection of, and active responses to malicious activity and ransomware attacks.
- **Product Usage Statistics** (*Opt-out*). Analyzes product usage patterns anonymously for continuous user experience improvements.
- **Support Channel** (*Opt-in*). Allows Cohesity technical experts to troubleshoot and remediate problems directly on your cluster.

You, as a Cohesity customer, control each of these channels. You can enable or disable any or all of them.

NOTE: If you are mandated by regulation or policy to prevent all communication outside of your organization's network, also known as a 'dark' or 'classified' site, disable all of the channels discussed here.

Figure 1: Cohesity Cluster Secure Phone-Home Communication Channels



All Phone-Home channels are encrypted between the cluster and Cohesity services. All those Cohesity services are located in the public cloud and have a secure login mechanism. The services are configured to accept connections only from the Cohesity cluster and authorized Cohesity personnel. All service access is restricted to a limited Cohesity staff, and a strict user registration policy is enforced and audited regularly.

Read the chapters below to learn about each channel's properties and default behavior, and how to manage them:

- **Default Status**. Is the channel *opt-in* or *opt-out* by default?
- **Communication Direction**. Is the channel traffic unidirectional or bidirectional?
- **Endpoint**. The endpoint to which telemetry data and metadata is sent from the clusters to Cohesity services.
- **Requires Port**. To use this channel, confirm that this port is open in your firewall.
- **Auditing**. Is the channel's activity captured in the audit logs?
- **Telemetry Data and Metadata**. Types of information sent to the service.
- **Can Request to Delete Data**. Can you request that Cohesity delete the data that was sent?

Each chapter also includes instructions on viewing the channel's current status and how to enable and disable it.

Manage Helios Support Automation and Proactive Wellness Channel

To help you meet your business requirements, the Helios Support Automation and Proactive Wellness channel detects issues and proactively opens Support cases when warranted. For example, if a disk in your cluster were to fail, this channel might automatically open a case with Cohesity Support, who would then reach out to you. To enable this, clusters send telemetry data and metadata at regular intervals to Cohesity services.

In addition to offering proactive support to customers, this channel produces insights to Cohesity for continuous product improvements.

This channel is enabled by default—that is, it works on an *opt-out* model.

The Helios Support Automation & Proactive Wellness channel's properties and default behavior are:

- **Default Status**: Enabled by default (*opt-out* model).
- **Communication Direction**: Cluster to Cohesity (*unidirectional*).
- **Endpoints**: The URLs where data, telemetry data, and metadata are sent from your clusters to the Cohesity service.
  - https://helios.cohesity.com
  - https://helios-data.cohesity.com
- **Requires Port**: 443 (HTTPS)
- Auditing: n/a
- **Monitoring**: The success or failure of the channel's send activity is logged in the system logs.
- Telemetry Data and Metadata:

This channel sends the following types of information from your cluster:

  - Alerts
  - Cluster config & status
  - Firmware information
  - A time capsule of the various cluster services
  - Audit logs
  - Statistics on capacity, performance, and more
  - Cohesity system settings
  - Rest API outputs
  - Debug logs
  - Linux command outputs

- **Can Request to Delete Data**: Yes. Contact Support.

View and Control Helios Support Automation and Proactive Wellness Channel Status

By default, the Helios Support Automation and Proactive Wellness channel is enabled (following an *opt-out* model). Use the Cohesity Platform CLI to view and manage the settings.

To manage the Helios Support Automation and Proactive Wellness channel, log in to your cluster as an administrator and:

- To **View** the current status of the channel, run:

```
$ iris_cli cluster info
```

In the output, look for `ACTIVE MONITORING ENABLED`. If true, the channel is enabled.

- **Disabling** this channel is version specific. For versions other than 6.6.x, run:

```
$ iris_cli cluster update-active-monitoring enable=false
$ iris_cli cluster info
```

After running the disable command, run the status command above again to confirm that `ACTIVE MONITORING ENABLED` is set to **`false`**.

- For version 6.6.x only, run:

```
$ iris_cli cluster update-gflag gflag-name="disabled_service_names"
gflag-value="pushclient" service-name=nexus reason="Disable push client
in 6.6.x* clusters KB6063"
$ allssh.sh "sudo systemctl restart nexus"
$ allssh.sh "pushclient.sh stop"
& allssh.sh "sudo systemctl disable pushclient"
```

> **NOTE**: This script is applicable only for 6.6.x and after an upgrade within version 6.6.x, you must re-run the above commands in listed order for the cluster to keep services in disabled mode.

- Verify the disabled status:

```
$ allssh.sh "pushclient.sh status"
     =========== <Node IP> ===========
     =========== <Node IP> ===========
```

Output will be empty as shown above If the channel is disabled.

Use Helios Global Active Management Channel

To enable you to manage all your clusters, data, and applications from a single view, Cohesity provides Helios, our global SaaS-based application management platform. It offers comprehensive active management of your data and applications wherever they reside: on-premises, cloud, and/or edge. In addition to multi-cluster management, Helios provides global monitoring, reporting, and fast, actionable search.

Cohesity Helios uses cutting-edge, machine-learning-based algorithms to detect and respond to cyber threats and ransomware attacks. Customers can use Helios Global Active Management to manage and enforce global protection policies and software upgrades on all Cohesity clusters from a single, aggregated view.

In addition to these benefits, this channel includes the Helios Support Automation & Proactive Wellness channel and all its features. This channel is disabled by default — that is, it works on an *opt-in* model.

> **NOTE**: Because the Helios Global Active Management channel relies on the information sent in the Helios Support Automation & Proactive Wellness channel, the *latter* must be enabled for *this* channel to work.

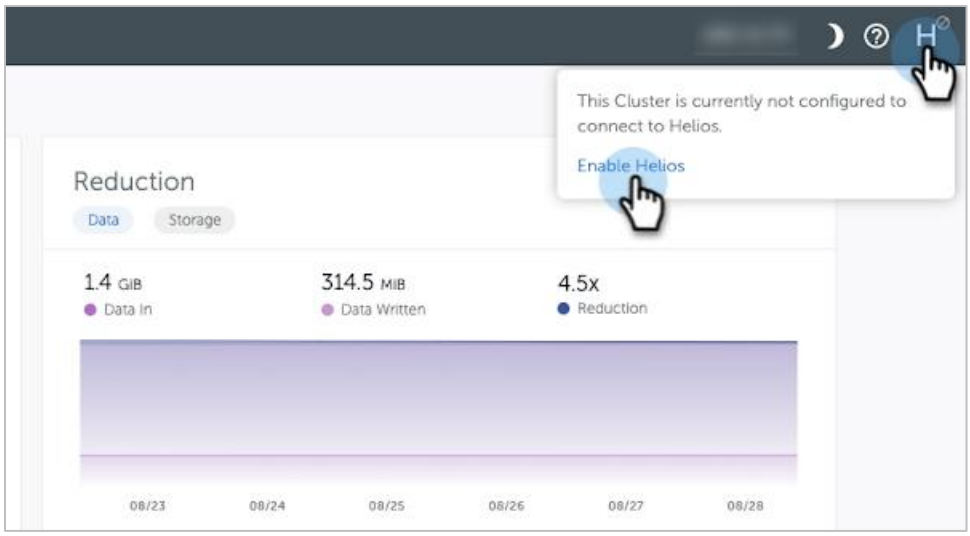
- The Helios Global Active Management channel's properties and default behavior are:
- **Default Status**: Disabled by default (*opt-in* model).
- **Communication Direction**: Cluster to Cohesity and Cohesity to cluster (*bidirectional*).
- Endpoints:
  - `https://helios-data.cohesity.com`
  - `https://helios.cohesity.com`
  - `https://google-analytics.com`
- **Requires Port**: 443 (HTTPS)
- **Auditing**: All customer user actions on the cluster are audit logged. Helios audit logs are *not* included.
  - If you unregister a cluster from Helios, Cohesity automatically deletes all the information *about* the cluster from Helios, but the cluster remains.
- Telemetry Data and Metadata:
- This channel sends the following types of information from your cluster:
  - Objects discovered from various registered sources, including External and Replication Targets.
  - License data on purchased SKUs.
  - Protection Group details and Protection Runs.
  - Dashboard, users, and groups activity.
  - All data sent by the Helios Support Automation & Proactive Wellness channel.
- **Can Request to Delete Data**: Yes. To remove all your data from Cohesity's systems, contact Cohesity Support.

View and Control Helios Global Active Management

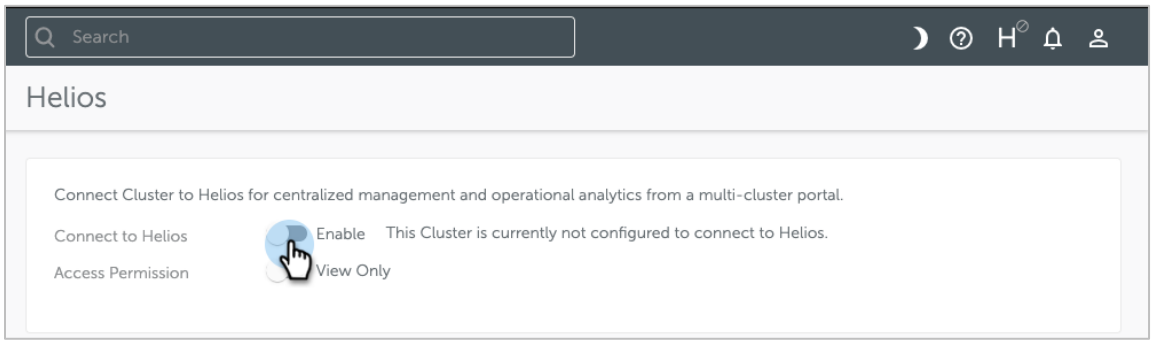
By default, Helios Global Active Management is disabled (following an *opt-in* model). Log in to Cohesity to view and manage the channel.

To enable Helios:

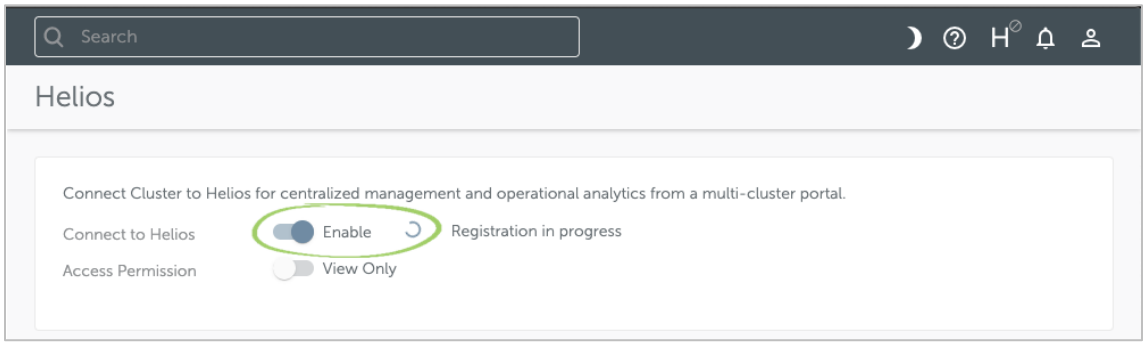
1. Log in to Cohesity. On the top right, click the Helios icon and select **Enable Helios**.



2. Next to Connect to Helios, click Enable.

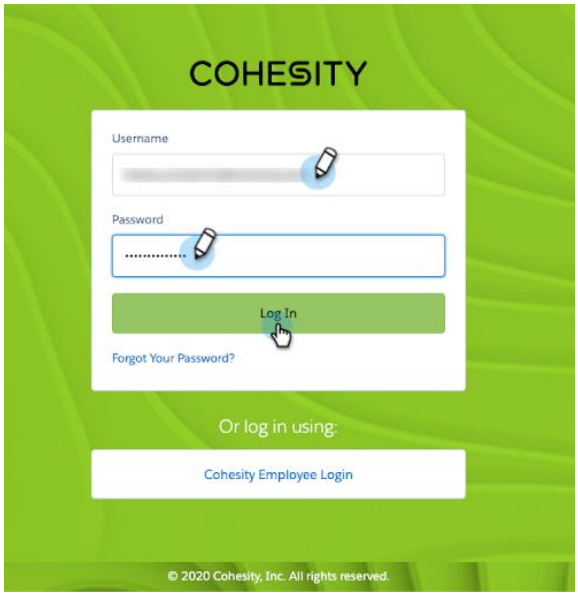


3. When you connect to Helios, the page displays the progress until the **Log In** window appears.

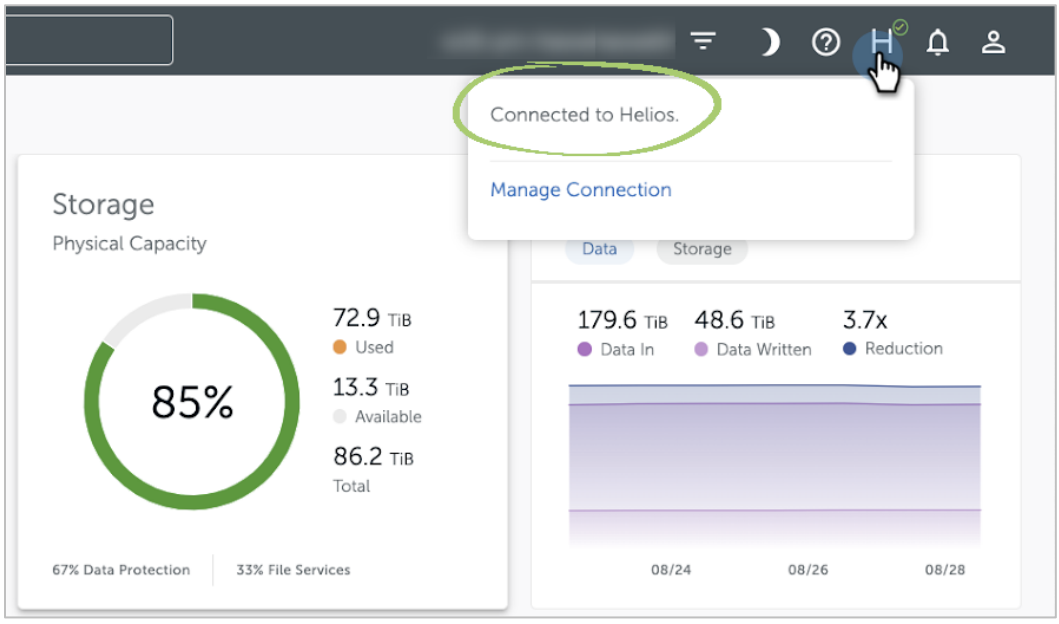


NOTE: Under **Access Permission**, if you enable **View Only**, everything from this channel will still work, but you will not be able to manage and enforce global Protection Policies and software upgrades from a single, aggregated view.

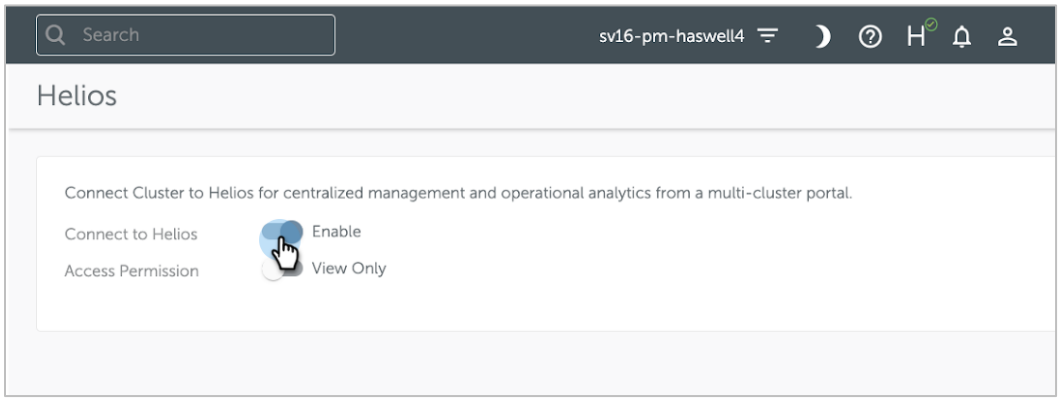
4. In the **Log In** window, enter your Helios credentials.



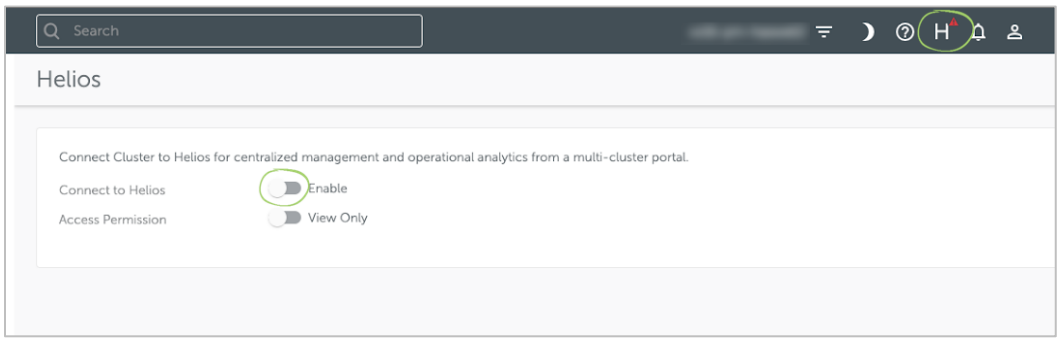
5. To view the current status of the channel, click the **Helios H**, and view the status.



6. To disable the channel, log in to your cluster, select the **Helios H** > **Manage Connections**, and toggle **Enable** to disable.



7. When you disconnect from Helios, the page shows **Enable** as *off* and the Helios icon shows the *disconnected* mark.



Manage Product Usage Statistics Channel

To continuously improve our users' experience with our product, Cohesity collects anonymized usage statistics for Cohesity from the browser. This helps us understand customer interactions and simplify the workflows in our products.

This channel is enabled by default — that is, it works on an *opt-out* model.

The Product Usage Statistics channel properties and default behavior are:

- **Default Status**: Enabled by default (*opt-out* model).
- **Communication Direction**: Browser to Cohesity (*unidirectional*).
- **Requires Port**: 443 (HTTPS)
- **Endpoint**: https://google-analytics.com
- Auditing: n/a
- Telemetry Data and Metadata:

This channel only sends browser information from your Cohesity sessions (and nothing from your cluster):

  - Pageviews
  - Page IDs
  - User navigation & flow

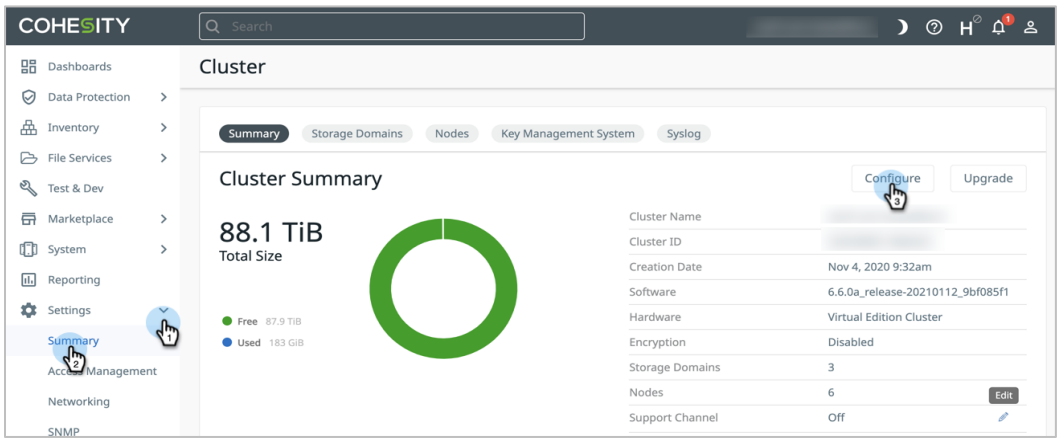
- **Can Request to Delete Data**: Not applicable, as the data is anonymized.

View and Control Product Usage Statistics Channel

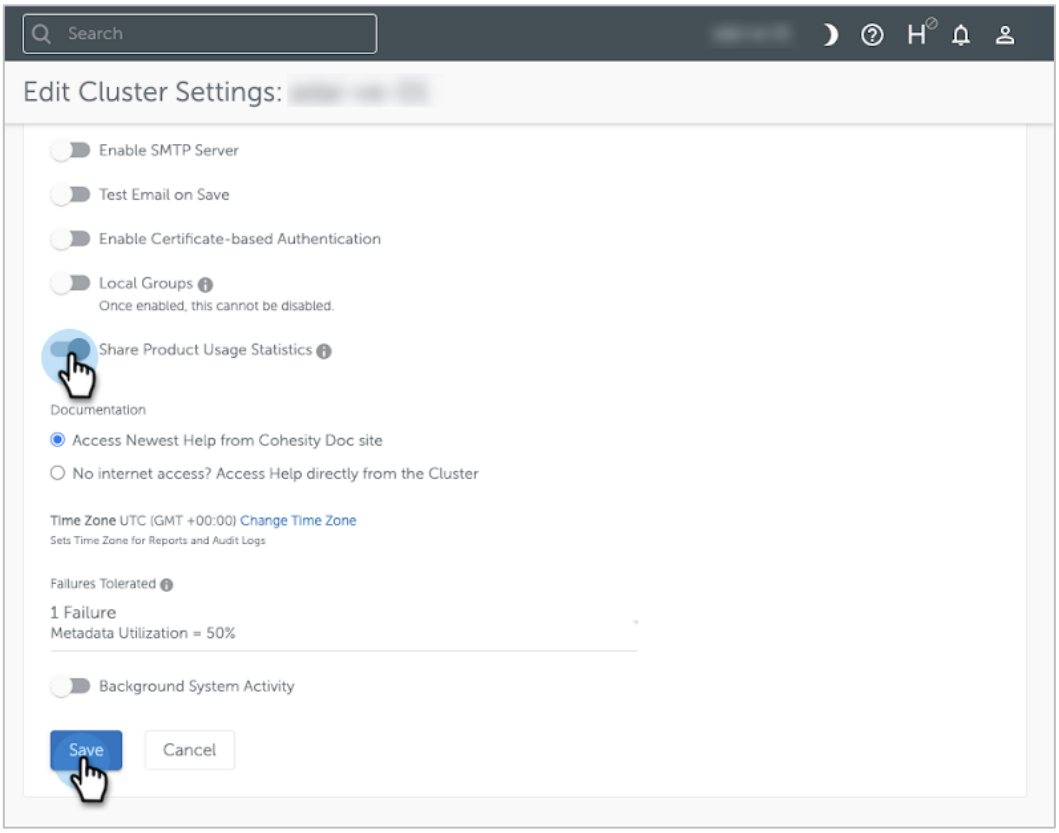
By default, the anonymized Product Usage Statistics channel is enabled (following an *opt-out* model).

To manage the channel:

1. Log in to Cohesity and select **Settings** > **Summary**. Click **Configure** above the cluster details.



2. Click Share Product Usage Statistics and Save.



Enable Support Channel for Remote Troubleshooting

To enable secure, on-demand, 'remote hands' assistance, you can open the Support Channel for Cohesity Support engineers to help troubleshoot issues. At times, our Support engineers might request that you open this channel so that they can log in to your cluster remotely to expedite a case's resolution, but the channel can only be enabled by you, the customer, and only temporarily (as of Cohesity 6.5.1b and above).

Our Support Channel service is located in the public cloud and has a secure login mechanism. The service can accept connections only from the Cohesity cluster and authorized Cohesity personnel. Access to the Support Channel is restricted to a limited set of Cohesity staff, and a strict user-registration policy is enforced and audited regularly.

This channel is disabled by default — that is, it works on an *opt-in* model, and only for the time that you leave it open for troubleshooting.

The Cohesity Support Channel's properties and default behavior are:

- **Default Status**: Disabled by default (*opt-in* model).
- **Communication Direction**: Cluster to Cohesity and Cohesity to cluster (*bidirectional*).
- **Endpoint**: Connects to

SOFTWARE VERSION	ENDPOINT SERVER	PORT
For version 6.6.	`rt.cohesity.com`	SSH 22
For version 6.8 and above	`Support-connect.cohesity.com` `support-connect-trust.cohesity.com`	TCP 443

- **Auditing**: All Support Channel usage is tracked and logged in audit logs.
- Telemetry Data and Metadata:

  This channel provides access to Cohesity Support staff and does not automatically send *any information* to Cohesity services. However, in troubleshooting your issue, Cohesity Support staff might access relevant information from your cluster, including:

  - Support logs
  - System settings
  - View job progress for problem diagnostics
- Can Request to Delete Data: Yes. Contact Support.

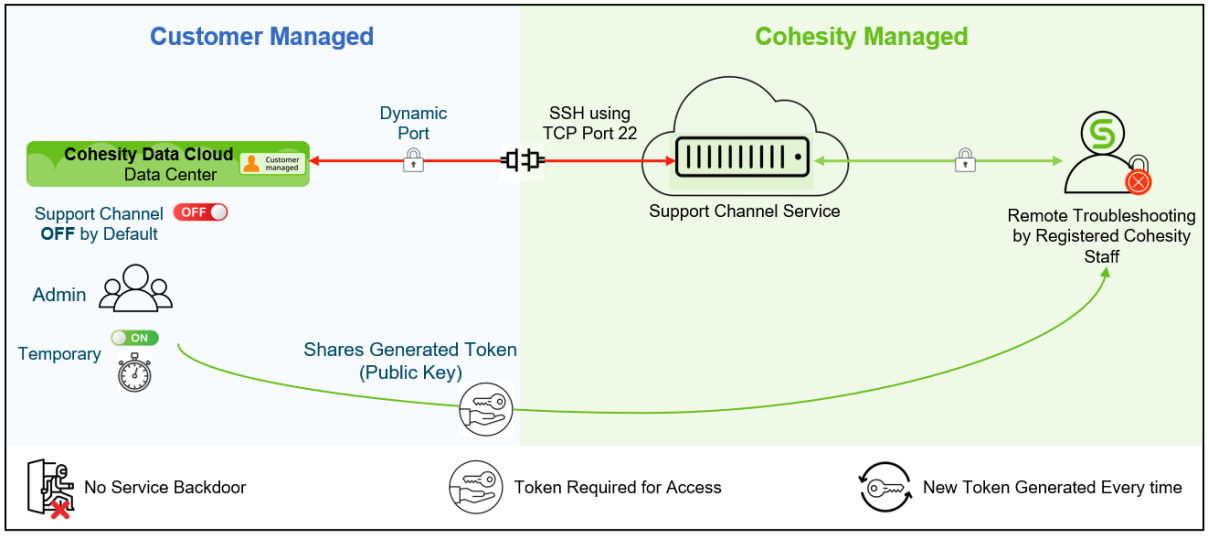
View and Control Support Channel

Use the Cohesity cluster login to view and control the Support Channel.

As of Cohesity version 6.5.1b, the Support Channel can only be enabled temporarily and the previous **On** option is no longer available. Also, access is protected by a token exchange. When you enable the Support Channel, a token is auto-generated. Before Cohesity Support engineers can log in to your cluster, you must share the token with them.

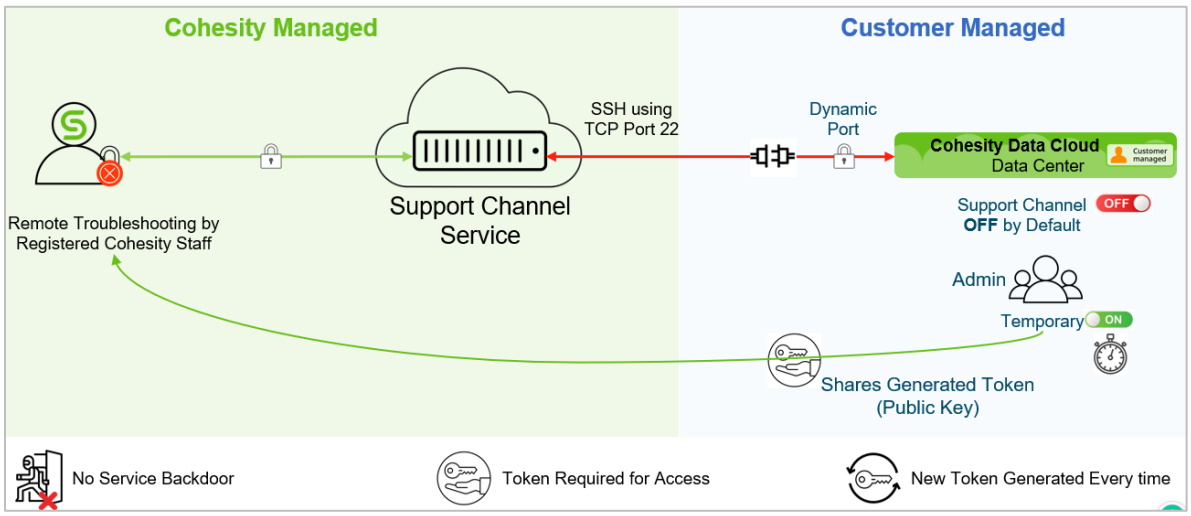
NOTE: The shared token works like public-private key setup — having access to the token by itself is not enough to log in

Figure 2: Support Channel Access Protected by Token Exchange (Cohesity 6.5.1b and above)



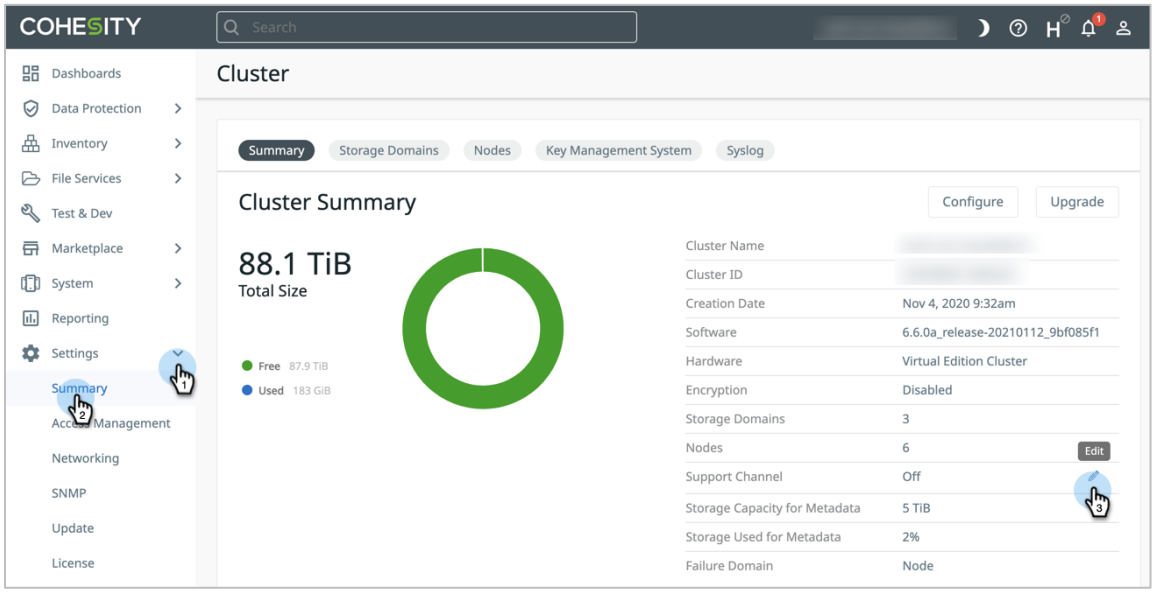
NOTE: From the 6.8.1_u1 release onwards, the RT server is deprecated and is replaced with the Teleport support server. The primary node in the cluster initiates an SSH reverse tunnel with the Teleport support server on TCP port 443.

Figure 3: Support Channel Access Protected by Token Exchange (Cohesity 6.8.1 and above)

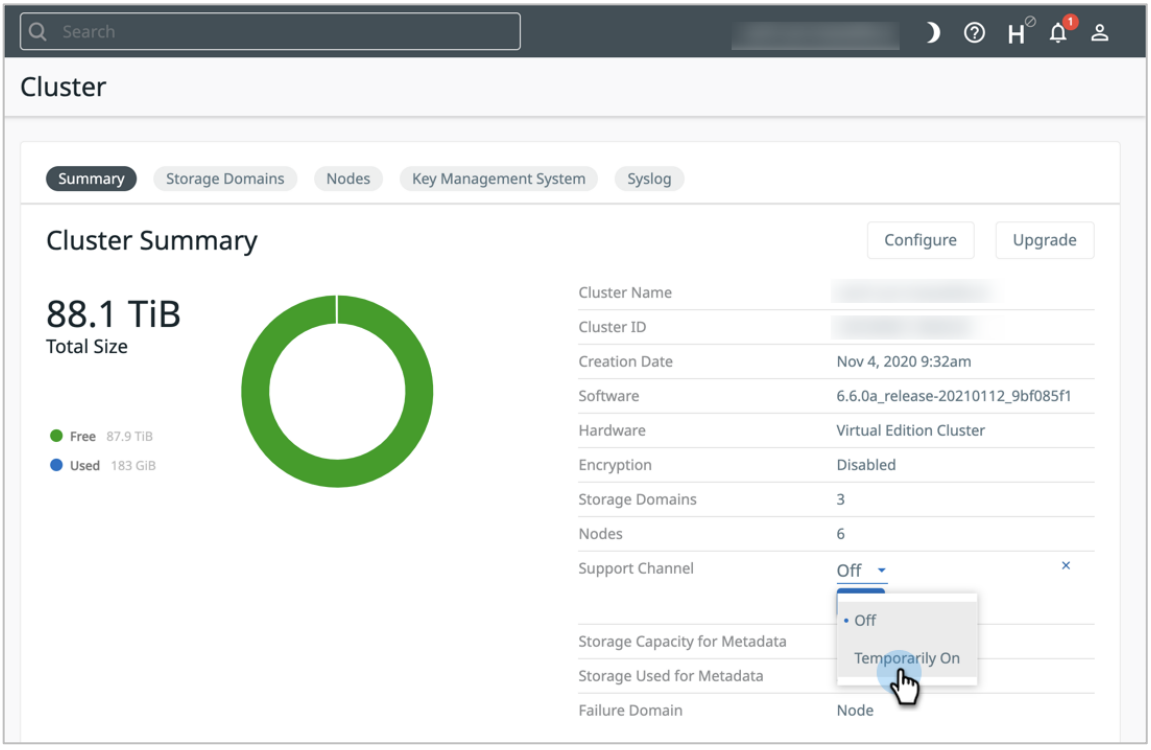


To use the Support Channel:

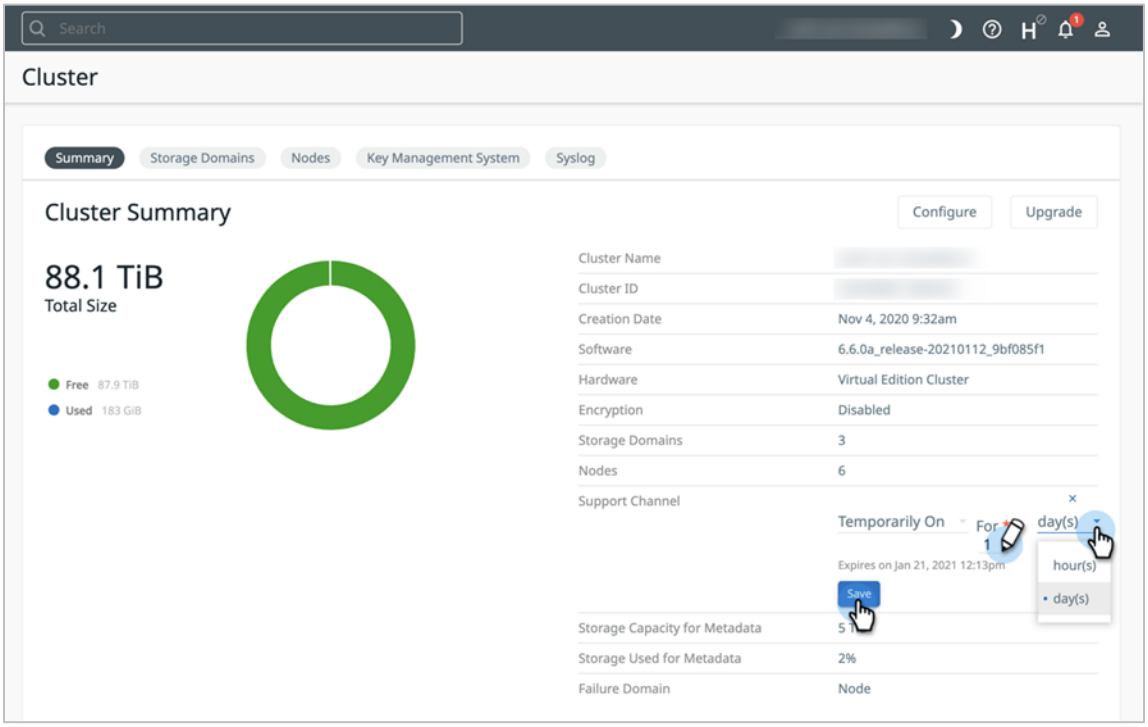
1. Log in to Cohesity and select **Settings** > **Summary**. On the **Support Channel** row, click the **Edit** icon.



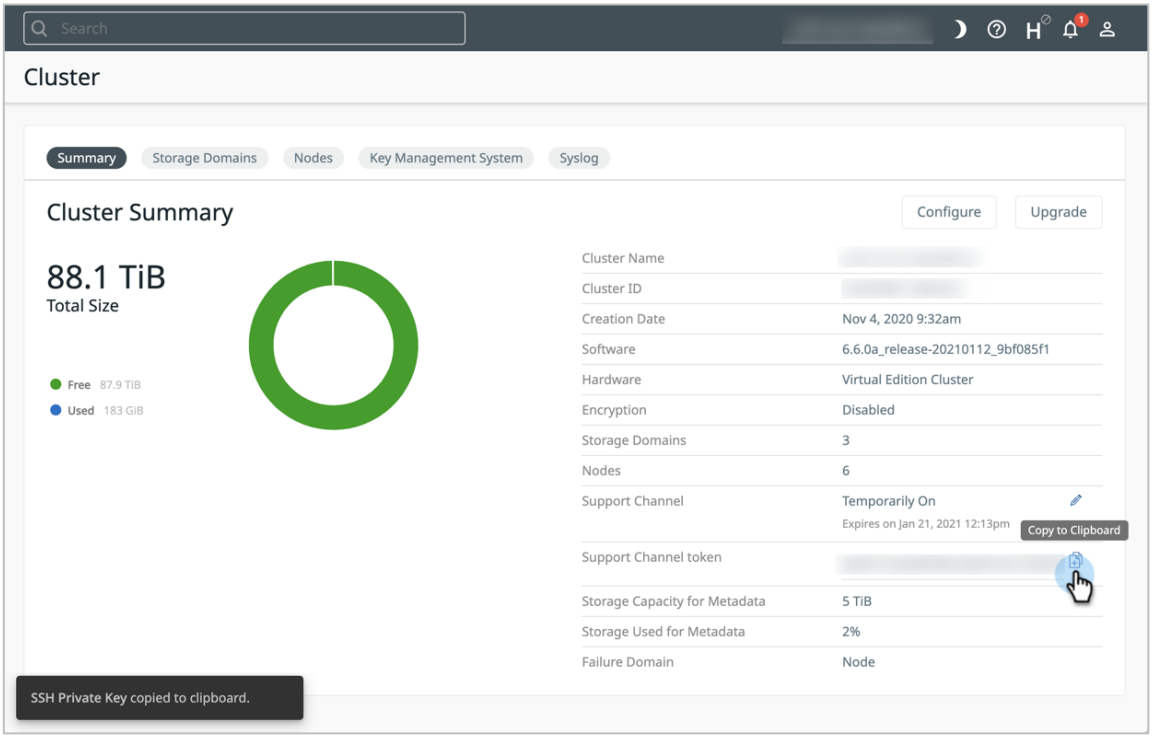
2. Select **Temporarily On**.



3. Set the period that the Support Channel should remain enabled and click **Save**. When you do, the Support Channel token is auto-generated.



4. On the **Support Channel Token** row, click the **Copy** button.



5. Send the token to the Cohesity Support staff who are troubleshooting your case to allow them to log in (temporarily) to your cluster.

6. Depending on Cohesity support assistance, set the time duration for the support channel. When the time duration you set for a support channel expires, the support channel token also expires.

   NOTE: In Cohesity versions before 6.5.1b, you can turn the Support Channel on permanently. For added security, Cohesity recommends you *only* use the **Temporarily On** option in those versions.

7. For more information on managing support channels, refer to Cohesity Product Documentation.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Adaikkappan Arumugam is Director, Product and Solutions at Cohesity. In his role, Adai focuses on connecting Cohesity's developer and product management staff's technical expertise with the needs and feedback from Cohesity's customers, support staff, and sales enablement staff.

Jason Hayes is Director, Information Security, at Cohesity. In his role, Jason focuses on the design and operations of the Cohesity Information Security Management System.

Other essential contributors included:

- Mark Mullenhoff, Sr Systems Engineer
- Ravi Murugan, Director, Engineering
- Sagar Sethi, Technical solutions Engineering

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.5	Sep 2024	Republishing
1.4	June 2023	Teleport server updates
1.3	Oct 2022	• Updated 6.6.x PushClient Disablement. • Removed Helios Licensing requirements. • Renamed guide to use the term phone-home.
1.2	Jul 2022	Minor update
1.1	Jan 2021	Minor update
1.0	Sep 2020	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.

© 2024. Cohesity, Inc. All Rights Reserved. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.