COHESITY

Cohesity Data Cloud Security Hardening Best Practices

Configure the Cohesity Data Cloud to Meet Your Security Requirements

Version 3.3

March 2026

ABSTRACT

In today's cyber-enabled world, establishing efficient and secure access to IT platforms is critical. With that in mind, this document aims to help IT operators, administrators, and architects implement key security principles that enhance confidentiality, data integrity, and controlled access to the Cohesity Data Cloud in customer-managed environments.

In this guide, we discuss the controls built into the Cohesity Data Cloud that—if implemented—will strengthen security and help safeguard the platform from multiple attack vectors. We also discuss best practices around some of these controls. This guide is designed based on Cohesity software version 6.6 (latest LTS). This document does not address security of Cohesity Software-as-a-Service offerings or Cohesity-managed environments; for information on those topics, please refer to the respective Cohesity documentation.

Table of Contents

Tables

Figures

Top Three Security Risks and Best Practices

Following are the top three security risks that modern-day enterprises face in the growing cyber-threat landscape:

- **Leaked or Compromised Credentials**—leaked or compromised passwords in a data-breach situation makes the user accounts vulnerable and enables attackers to gain access to your cluster.
- **Data Loss**—data exfiltration or data deletion, which can be intentional or accidental.
- **Data Exposure**—exposure of sensitive information due to elevated access.

To help address these risks and others, follow the detailed Cohesity security hardening checklist provided in Appendix A.

Upgrade to Latest LTS Release Version

Cohesity recommends keeping your cluster up to date with the latest LTS release and patches available at downloads.cohesity.com. Cohesity is committed to security and releases frequent patches to vulnerabilities. Keeping your software up to date is critical in ensuring that vulnerabilities are addressed on time.

Read the release notes for all the critical information about upgrading to a version. You can also upgrade the cluster with the latest version from the Cohesity cluster at **Settings** > **Summary** > **Upgrade**.

For more information, see Cohesity product documentation.

Secure Your User Account and Password

Securing a Cohesity cluster involves creating the default password policy and changing the default user account passwords. The Cohesity Data Cloud comes with the following default user accounts to help you access the Cohesity UI, Secure Shell (to restrict SSH access to the host operating system shell), and the Cohesity console.

Table 1: Default User Accounts

USER ACCOUNT	USER TYPE	PURPOSE
Admin	User interface	Access to Cohesity dashboard, API, and CLI
Support	Linux Shell	Access to Cohesity Secure Shell with limited access
Cohesity_console	Console	Access to Cohesity console
Root	Console	Access to Cohesity console In DoD mode only
IPMI (Intelligent Platform Management Interface)	Interface	Remote access to IPMI interface prompt, console prompt, and other IPMI tools with Split key feature

NOTE: The Linux user account 'Cohesity' is deprecated. Use the 'support' user account for shell access. From version 6.8 onwards, Secure Shell is enabled, which restricts SSH access to the host operating system shell, further tightening access to the Cohesity cluster.

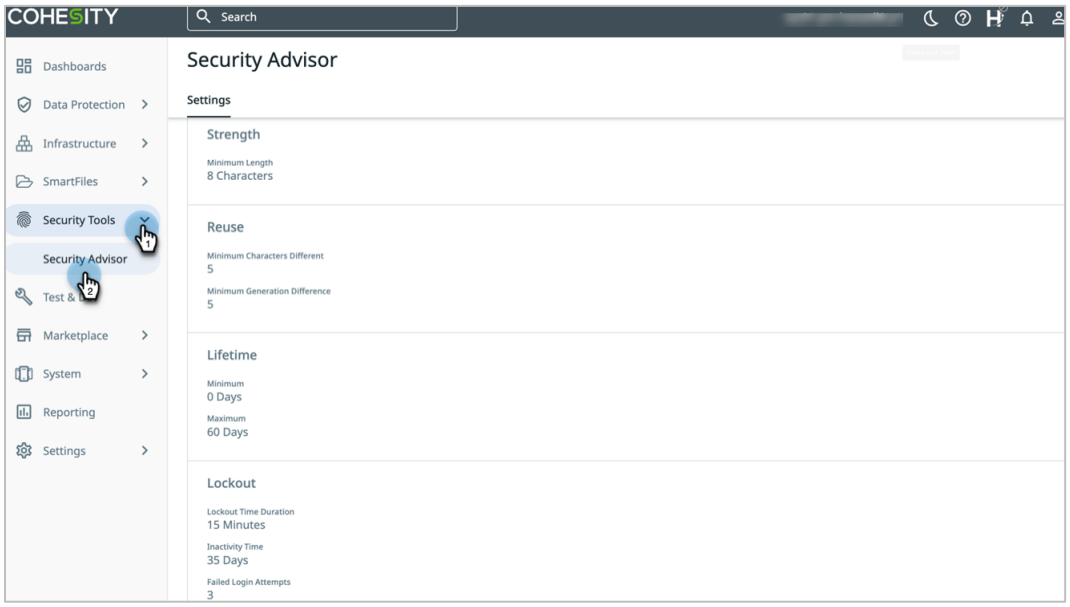
Cohesity recommends keeping the Secure Shell enabled, which will limit access to the root user.

Update the Default Password Policy

The default password policy is assigned to all the local user accounts. Update the default password policy in accordance with your own organization's requirements, standards, and best practices.

- **Password Strength**—password length must be a minimum of 8 characters by default. Depending on your organization's policy, you can choose to increase the number of characters and enforce a combination of upper case, number, and special characters for added security.
- **Password Reuse**—by default, you cannot reuse the last five passwords. Configure the 'reuse password' to meet your organization's requirements and standards.
- **Password Lifetime**—password expiry is set to 60 days by default. You can choose to increase or decrease the password expiry as per your organization's policy.
- **Account Lockout**—by default, three consecutive failed login attempts lock the user account. You can choose to modify the failed login attempts, lockout duration, and inactivity time.

To update the default password policy, navigate to **Security Tools** > **Security Advisor**. For more information, see Update Default Password Policy in Cohesity's product documentation.



Update Default User Passwords

As a security best practice, you must change the default password of your Cohesity clusters before starting the operations. This helps minimize the likelihood or impact of an attack and keeps the data secure.

The following section outlines the procedure to change passwords for local users on the Cohesity Data Cloud:

- **Change 'admin' user password**: The Cohesity cluster is configured with a default system administration user called 'admin'. This user has the same privileges as a user with the admin role. Cohesity strongly recommends you change the default password. Cohesity prompts you to change the default password the first time you log in. For directions to change the admin password, see Change Local User Password.
- **Change 'support' user password**: By default, the 'support' user is disabled. You should enable the 'support' user account to access the Cohesity shell and set the strong 'support' user password from the cluster user interface or using the `iris_cli` command. For directions to change the 'support' user password, see Manage Support User.

NOTE:

- For security reasons, sudo access is disabled by default for the 'support' user. See Cohesity product documentation to enable or disable sudo access for the support user.
- From version 6.8 onwards, you can enable Secure Shell, which restricts SSH access to the host operating system shell, further tightening access to the Cohesity cluster. You can access it using the 'support' user account. For more information about the Enabling Secure Shell feature, see Cohesity product documentation.

- **Change 'cohesity_console' user password**. Cohesity version 6.5.1b introduced the 'cohesity_console' user account as a failsafe mechanism. If you are locked out of the cluster, have lost connectivity to the cluster, or have forgotten your 'support' user password, the 'cohesity_console' user is used to reset your Linux user password.

  To change the 'cohesity_console' user password, run the following command from the Cohesity shell:

  To set a new password:

  ```
  [Support@nodeIP]$iris_cli
  admin> user linux-user linux-username=cohesity_console
  linux-password=<password min 15 characters>
  ```

  To update a password:

  ```
  [Support@nodeIP]$iris_cli
  admin>user linux-user linux-username=cohesity_console
  current-password=<password min 15 characters>
  linux-password=<password min 15 characters>
  ```

- **Change 'root' user password**. For DoD mode, console access to the Cohesity nodes is available by login via the 'root' account. If you are locked out of the cluster, have lost connectivity to the cluster, or forgotten your support user password, you can reset your user account's password using the 'root' account user. You can change the root account password after enabling the cluster in DoD mode.
- **Change IPMI password**. The Intelligent Platform Management Interface is the out-of-band management port for Cohesity nodes. The IPMI user is established when you first set up your cluster. For directions to change the IPMI password, see Manage IPMI Configuration in the online help.
- **BIOS password and securing underlying servers**. An attacker could directly destroy your hardware with unfettered physical access. IPMI or the other remote maintenance tools may provide a means of taking control of the server by loading a different boot image, or depending on the vendor, directly accessing disks. To mitigate this risk, use secure methods such as a boot control password unknown to the backup admin or the admin of the production systems. Segregating network control is also effective. BIOS password is set only for Cohesity Data Cloud.

- **Keep your credentials safe and secure**. Keep all your Cohesity account credentials (admin, support, cohesity_console, root, console, IPMI) secure and safe using encrypted password vault platform (PIM/PAM) or key store to minimize the risk of password-based cyberattacks. Consider using a different PIM/PAM or key store solution for Cohesity accounts than you use for accounts governing production systems, so that in a worst-case scenario where a PIM/PAM system is compromised, such compromise impacts production or backups but not both.
- **Do not allow the same person to have the credentials for both the admin and support users**. To prevent dangerous unilateral actions by one rogue person, Cohesity enables the separation of the ability to enable sensitive support operations, which require sudo access. A person with access to the admin credentials should not have access to the support credentials or the cohesity_console credentials, and vice versa, so that no one person can take unilateral action to undertake sensitive support operations via the SSH support login.

  From Cohesity version 6.8 onwards, no combination of customer personnel can undertake sensitive support operations via SSH without obtaining temporary one-time-use approval from Cohesity support personnel.
- **Do not allow the same person to both reach the hardware layer and login to it unassisted**. People with physical access to the datacenter, or network access to the hardware layer via the IPMI card or similar out-of-band hardware management card, should also have the password to, from there, login to the Linux console.

  Cohesity supports this level of protection by giving users the ability to customize the console password. Similarly, those able to login to the IPMI card or equivalent should not already have the boot password needed to load an alternate boot image to re-provision the hardware. Hardware vendors similarly allow customizing an IPMI (or equivalent) boot password to prevent unauthorized alternate booting and subsequent reprovisioning of hardware.

Enable Native Multifactor Authentication (MFA)

Multifactor authentication is an additional layer of security used to verify the identity of a user. For enhanced security, Cohesity strongly recommends you enable MFA for all users and groups, including local users, AD users, and SSO users.

Administrators can select one or both of the following authentication methods:

- **Authenticator App**: Cohesity recommends you install a Time-based One-Time Password (TOTP) authenticator app such as Okta Verify, Google Authenticator, Microsoft Authenticator, Duo Mobile, etc., on your device and enter the verification code generated by the app.
- **Email**: Users must enter the verification code sent to their email address.

Ensure you enable the MFA for both ‘admin’ and ‘support’ user accounts. For more information, see Multifactor Authentication for Local Users and Multifactor Authentication for the Support User Account.

Microsoft Active Directory (AD) Setup

Depending on your organization's policy, you can choose to join the Cohesity cluster to one or more Active Directory domains. To join your Cohesity cluster to an Active Directory domain, follow the procedures in our Join Active Directory product documentation. Cohesity also strongly recommends adhering to the following security best practices for Active Directory users.

- **Create Role-based Access Control (RBAC) for AD users**: Ensure you create the least privileged roles ('Operator' or 'Self Service Data Protection') to perform the backup and restore workflow.

  > **NOTE**: Avoid granting, managing, or modifying privileges to any of the AD users.

- **Create a separate service account**: For Cohesity operations, create a service account in AD, which is different from the user's generic AD account. This will further protect the Cohesity environment in case the user's generic AD account gets compromised.
- **Enable MFA for all domain users (applicable from Cohesity version 6.8 and above)**: Set up a two-step verification method to authenticate users and control access.

See Cohesity product documentation to join the Cohesity cluster to AD Domain, add AD users and groups, and create user roles.

Integrate with Single Sign-On Identity Provider (IdP)

You can configure Single Sign-on IdP, to increase compliance and security, simplify user management, streamline user access to Cohesity operations and objects, and improve auditing. Cohesity supports SAML 2.0 & OpenID Connect based Single Sign-On and major IdP vendors such as Okta, Duo, Ping, and Azure AD and Microsoft Entra ID.

- **Add the IdP to the cluster**: Once you create an application in the identity provider for the Cohesity cluster, configure the IdP SSO URL and the X.509 certificate file in PEM format.
- **Configure less privileged roles for SSO users**: You can add SSO users to the Cohesity cluster after creating an application in the identity provider for the Cohesity cluster. Ensure you create less privileged roles for the SSO users, for example, 'Operator' and 'Self Service Data Protection' roles.
- **Default role for all SSO users**: An option provided while configuring SSO IdP on your Cohesity cluster. Ensure you choose a 'Viewer' role for any SSO user who logs in to the Cohesity cluster.
- **Enable MFA on SSO provider**: Cohesity highly recommends enabling MFA with your SSO provider to authenticate SSO users through a two-step verification process and enhance security.

Securing BMC Access

Here are some suggestions and best practices to secure out of band BMC access:

Table 2: Suggestions and Best Practices

Measure	Benefit	Risk/Challenge
Physically disconnect BMC network cable	Most secure	Most manual; difficult for remote sites
Shut switch ports down when not in use	Easier to manage remotely; able to route through change approval process, logging, alerting	Potentially vulnerable to attack if switch infrastructure is compromised
Unique passwords on each node	Limits damage from compromised credentials	More complex to manage; possible risk related to password manager
BIOS password	Mitigates certain attacks	More complex management
Configure phishing-resistant MFA anywhere possible	More secure	Not always available; shared accounts
Change default admin account name	Makes certain attacks more difficult	Not always possible
Perform vendor-specific actions, (DIP switches, etc.)	Well-validated	Varies between vendors; may disable other functionality; not always available
Assign BMC IP addresses in an isolated subnet, and limit which specific systems can access that VLAN	Less exposure for attacks	More complex network management
Enable logging for BMC access, and send events to a remote system	Better visibility to low-level access to systems; preserves evidence in the case of an attack on the system	Requires analysis of logs to see a benefit

Measure	Benefit	Risk/Challenge
Externally collect alerts for administrative logins to BMC interfaces, and give them higher priority	Raised awareness to hardware-level access of systems	Dependent on customer environment; can contribute to alert fatigue if too many alerts are generated
If possible, disable IPMI over LAN access	More secure	Requires physical access to the system to interact at the BOIS or console level

Manage User Roles

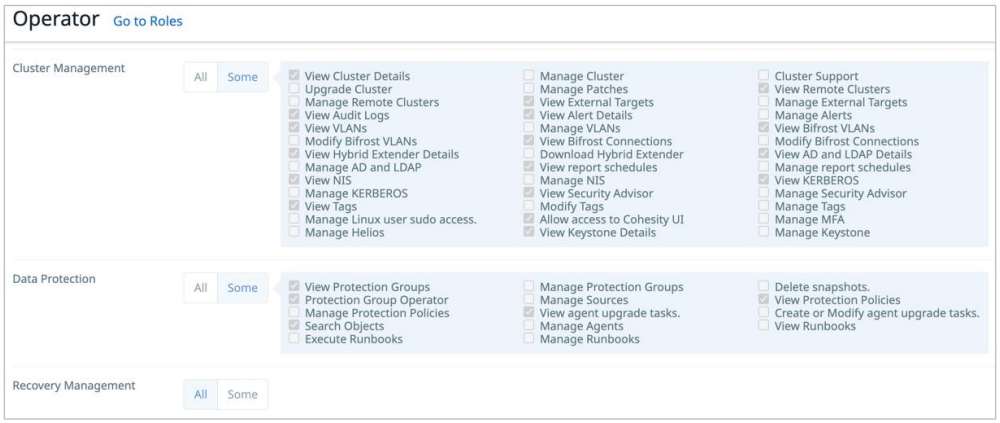
Authentication is required for all management methods (the Cohesity dashboard, CLI, and API). Only a user with an account on the cluster can authenticate to the cluster. You can create users and assign privilege levels to the users by assigning them different roles.

Cohesity Role-based Access Control

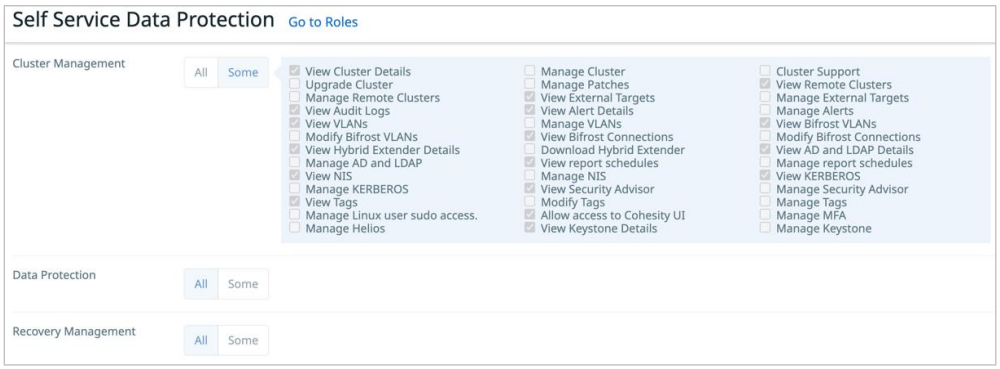
One of the foundational elements of a 'Zero Trust' framework is to provide minimal privilege access. Cohesity Role-based Access Control (RBAC) framework allows the admin to choose the proper privilege for a user to perform certain operations. By default, Cohesity creates eight pre-defined system roles. For more details, see Managing Roles.

For data protection users, ensure you have the following less-privileged roles assigned to the users who will perform the backup and recovery operations.

- **Operator Role**—Assign the 'Operator' role to the users with viewer privileges and can run the existing protection groups and recovery workflow.



- **Self Service Data Protection Role**—assign the 'Self Service Data Protection Role' to the users who create and manage protection policy, protection group, cloning, recovery, and Cohesity Views.



To create a customized role, follow the procedures in Cohesity product documentation.

Secure Your Automation and Integration

Customers can use the Cohesity APIs to automate their backup and restore workflows and integrate with other management products. Before making any API requests, the first step is to get the access token by making a 'POST/public/accessTokens' request with valid Cohesity credentials. The access token generated is valid for 24 hours.

Follow the below best practices to secure the Cohesity API integration:

- **Create a user account for automation**—Cohesity strongly recommends creating a new user account for automating your backup and recovery workflow.
- **Configure minimal privileged access for automation user account**—choose the 'Operator' or 'Self Service Data Protection' role for the user account to perform the automation. If needed, create a custom role, and choose the privileges needed for automation. Ensure the automation account does not have 'manage' access to DataLock, object deletion, and data security.

Secure Your Certificates

Signed certificates are essential to avoid man-in-the-middle attacks. Depending on your organization's Information Security Policy, you can choose to have self-signed or Certificate Authority (CA)-signed certificates. Cohesity clusters support X.509 certificates in PEM format and ship with an auto-generated self-signed certificate.

Configure Self-signed or CA-signed Certificates—Cohesity supports X.509 certificates with RSA 2048 or 3096 RSA signature and SHA-256 and SHA-384 hashing. Cohesity recommends configuring the certificates using SHA 384 hashing with RSA 3096 key algorithm.

Configure Cohesity CA Issued Certificate— From Cohesity Data Cloud version 7.1 onwards, Cohesity Certificate Authority Service (ca_exec) issues a unique CA cert/key for each cluster [Agent]. This unique CA cert/key is for Agent-to-Cluster communication and Replication communication. With support of **Intrinsic Automation**, existing agents are automatically provisioned new certs from the Cohesity CA. This avoids issues due to expired agent certificates that could cause a disruption in service.

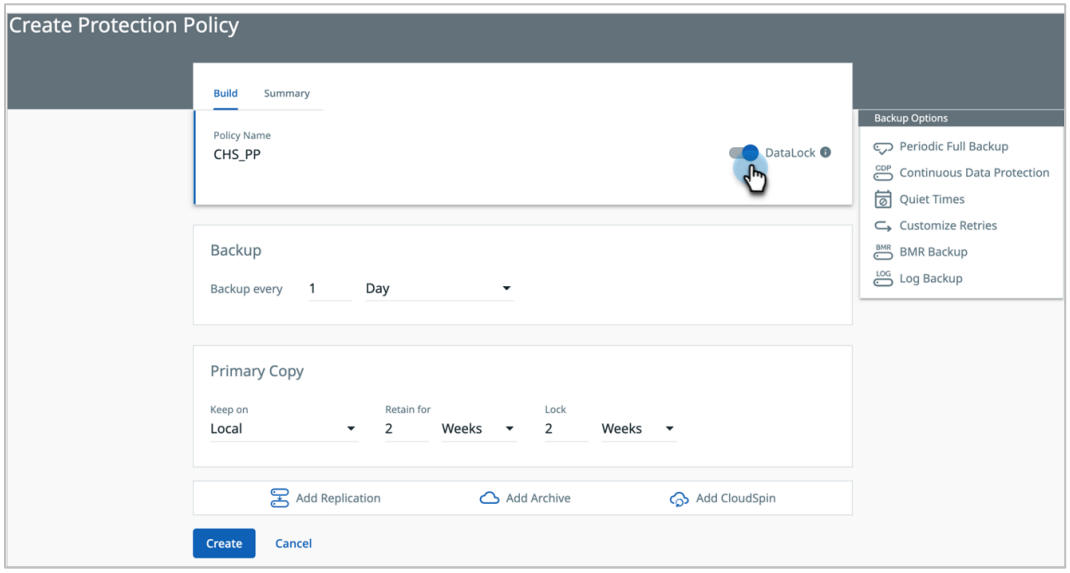
For more information, refer to Cohesity product documentation.

Secure Data Management

Enable DataLock

One of the most common cybersecurity attack vectors is to delete the backup. To help prevent malicious or accidental file deletion, Cohesity has DataLock, a WORM (Write Once Read Many) feature that prevents erasing backups intentionally or accidentally. It helps ensure that your data, including local backups, archives, and replication, are not modifiable until the DataLock expires. Once applied, you can delete a DataLocked snapshot only after its DataLock retention period expires, and it prevents all users from deleting any snapshots that were generated by a Protection Group. Only users with the authorized Cohesity Data Security role can add, modify, or remove a DataLock for future backups. However, no user of any kind can reduce the retention lock period for previously locked backups.

Cohesity strongly recommends enabling DataLock for additional security layers to secure your data. You can enable the DataLock while creating the Protection Policy. In Cohesity version 6.8, the DataLock is enabled by default.



NOTE: Even a Cohesity cluster administrator cannot delete or modify WORM-protected data.

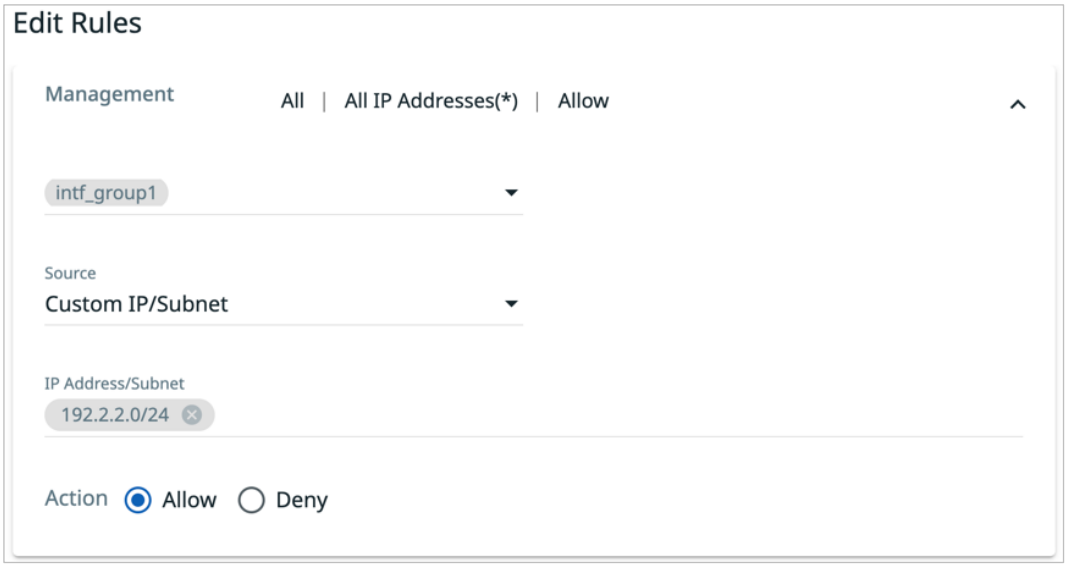
Secure Access Control

Configure Cohesity Firewall Profiles

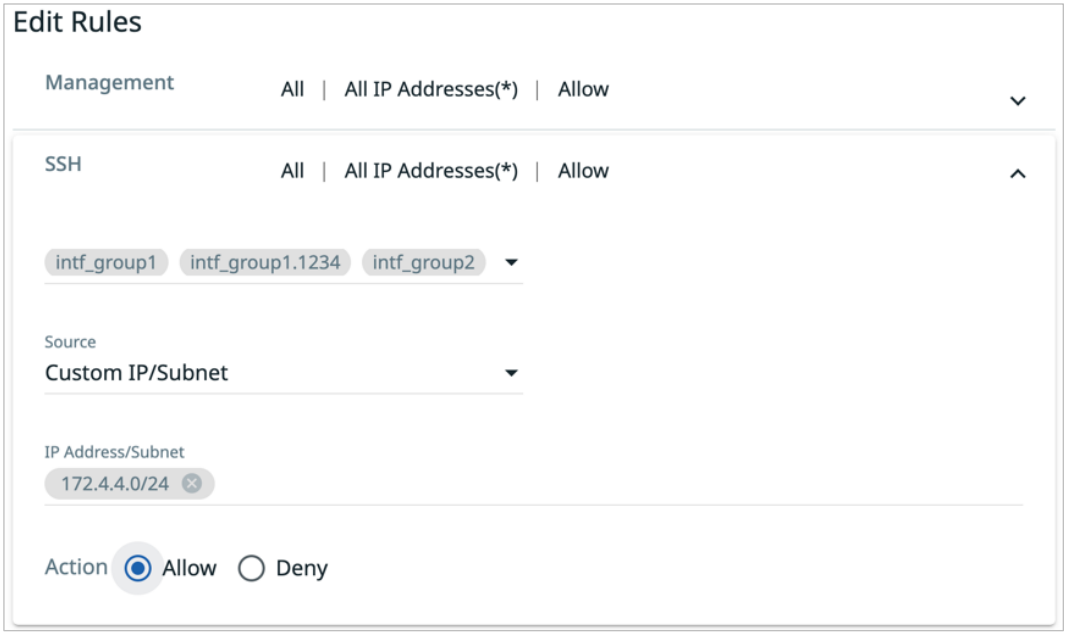
One of the most effective ways to secure access control is to restrict network access. Cohesity allows users to configure firewall profiles to restrict the incoming traffic on a Cohesity cluster. The Cohesity firewall profiles are application-based firewall rules that allow or deny the incoming traffic to the Cohesity cluster from specific IP addresses, ports, applications, and protocols. The firewall rules are applied to the Cohesity network interface (via interface_group) to secure incoming traffic at the network interface level.

As a security best practice, configure the following firewall profiles:

- **Management**—allow only the IP addresses of your systems that want to access Cohesity cluster web UI (HTTP/HTTPS traffic). The 'management' firewall profile applies the rules on TCP ports 80 and 443. This will prevent an attacker from accessing your Cohesity cluster from unknown IP addresses.



- **SSH**—allows only the IP addresses of your systems to access the Cohesity secure shell and applies the rules on port TCP 22.



NOTE: Configure the firewall profiles based on the application, protocols, and ports that you want to allow or deny.

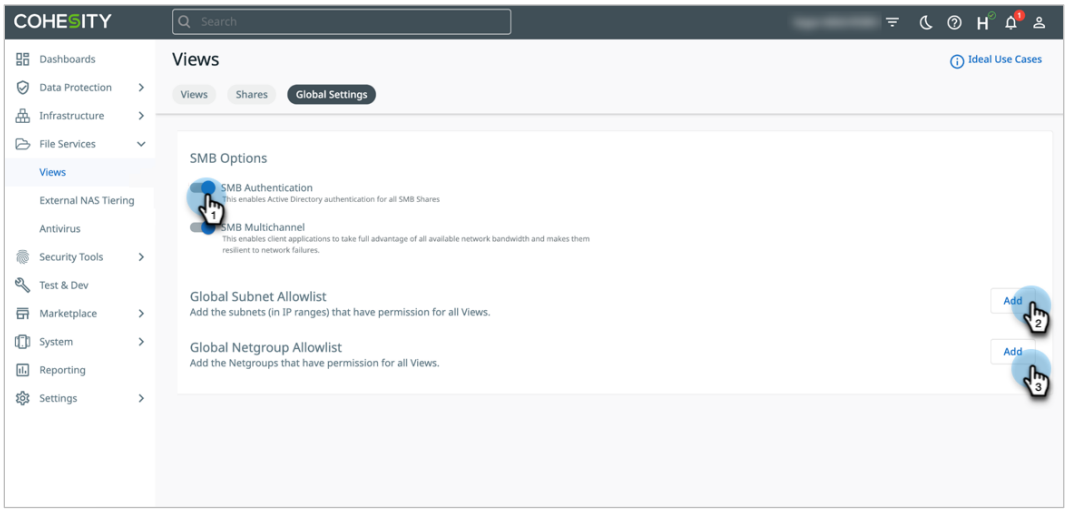
Navigate to **Settings** > **Networking** > **Firewall** to configure the application-based firewall rules. For more information, see Cohesity product documentation.

Secure Your Cohesity File and Object Services

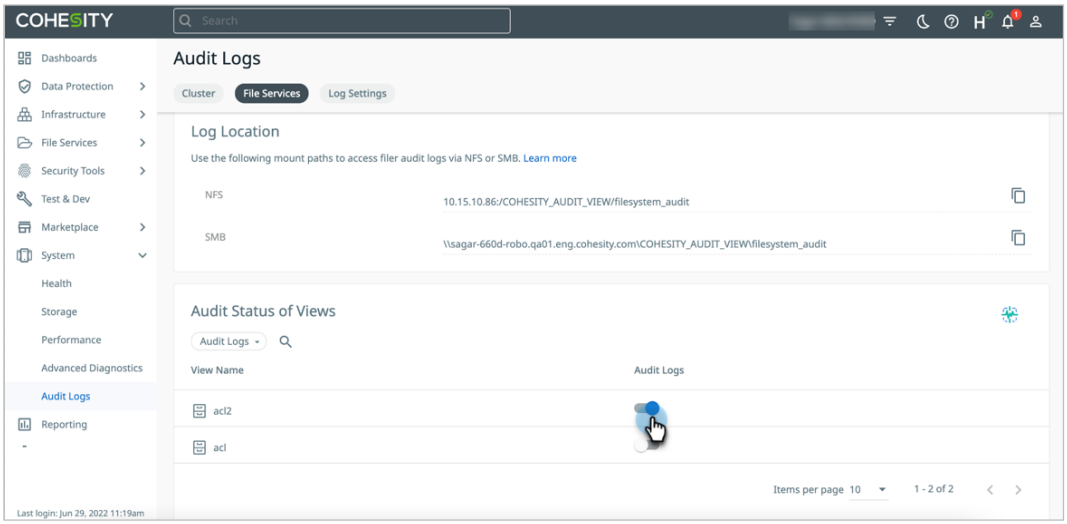
The Cohesity cluster can be used as file shares, backup targets, and object services. You need to create Cohesity Views that can be accessed using NAS protocols (NFS and SMB) or S3 object storage. Ensure you secure and restrict access to the Cohesity Views.

- **Create Global Allowlist**—configure the IP subnet of the systems that need access to the Cohesity Views. This will prevent unauthorized systems from accessing the Cohesity View.
- **Create View Allowlist**—narrow down the access list by configuring the IP address of the systems that need access to the Cohesity Views. You can override the global allowlist you configured in the above step.

- **Create Share Allowlist (SMB and S3)**—restrict access to the systems to mount and access the folders and subfolders in the share.



- **Enable Audit Logs** for Cohesity Files and Object Services.



- **Enable File DataLock**—depending on your organization's policy, you can choose to enable the File DataLock.
- **Enable File Filtering**—you can enable the File Filtering option to allow or deny specific file types, such as encrypted ransomware file extensions, to write to the Cohesity View. This will prevent unknown file extensions from getting written to the Cohesity View.

For more information, see add subnets to allowlists.

Set Web Session Inactivity Timeout and Session Limits

Configure your Cohesity cluster UI browser session as per your organization policy.

- **Web Session Inactivity Timeout**: The default session inactivity timeout value is 3600 seconds, and the session absolute timeout is 86400 seconds. You can configure the Cohesity cluster UI per browser session timeout period as per your organization's security policy.

```
iris_cli security-config update session-inactivity-timeout=<timeout
seconds>
iris_cli security-config update session-absolute-timeout=<timeout
seconds>
```

- **Limit Sessions**: By default, there is no limit on the active sessions allowed per user and concurrent sessions. Cohesity strongly recommends enabling the session limit. Set the value for the session limit per user as per your organization's policy.

```
iris_cli security-config update limit-sessions=true
iris_cli security-config update session-limit-per-user=<# of sessions>
```

Cohesity recommends changing the session timeout settings as per your organization's policy by logging through the support user account and changing the security config. See Security-config CLI options to update the different time values.

NOTE: Ensure to enable the session management before setting the timeout period. Contact Cohesity support to enable the feature.

Enable Login Banner

When you log into the Cohesity cluster, the first thing you see is the login banner. A best practice is to enable the login banner and create your banner, which can be a warning message that reinforces policy awareness during the login process.

For example:

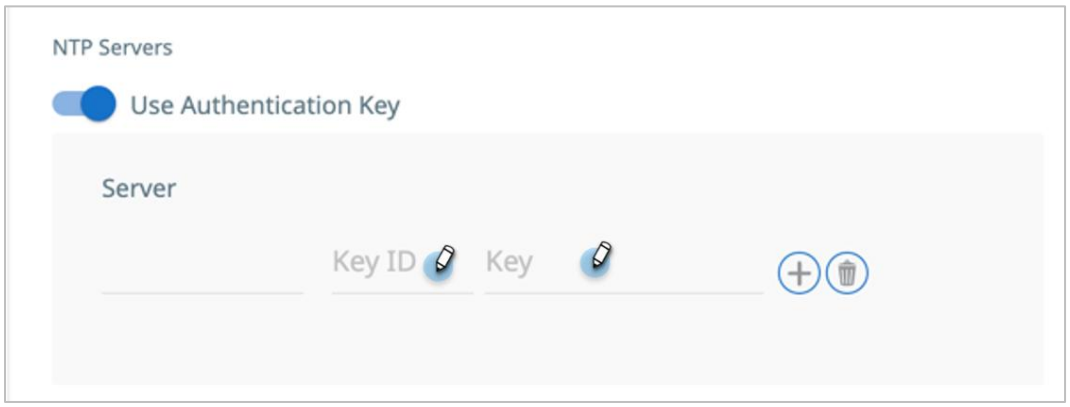
```
ssh support@10.x.x.x
support@10.x.x.x's password:

**************** Welcome to Cohesity *****************

WARNING: Unauthorized access to this system is forbidden.
By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.

*****************************************************
```

For more information, see Cohesity product documentation.

Configure Network Time Protocol (NTP)

The Cohesity Data Cloud is designed to operate in an environment where time can be reliably and securely established. The Data Cloud supports NTP and implements several defenses and in-depth techniques designed to ensure the platform can securely utilize trustworthy NTP sources. Most importantly, even if NTP keeps frequently hopping ahead of real time, the cluster will not allow cluster time to advance at a rate faster than 10 extra minutes per 14 days, making any impact on DataLock protection negligible. These techniques help prevent malicious manipulation of NTP and other time-based attacks that might enable premature removal of DataLock protection from backup snapshots and protected Views.

Use the Authentication Key to secure communication between the NTP server and the Cohesity cluster. In the **key ID** field, enter the Key ID associated with the SHA-1 key, and in the **Key** field, enter the SHA-1 key. To configure NTP, on the Cohesity UI, navigate to **Settings > Summary > Configure**.



For more information on NTP configuration and verification, see the docs section.

Enable Encryption

To protect your data from multiple attack vectors, Cohesity Data Cloud leverages a strong FIPS-approved AES 256 encryption algorithm for data at rest and TLS v1.3 with strong ciphers for securing data-in-transit.

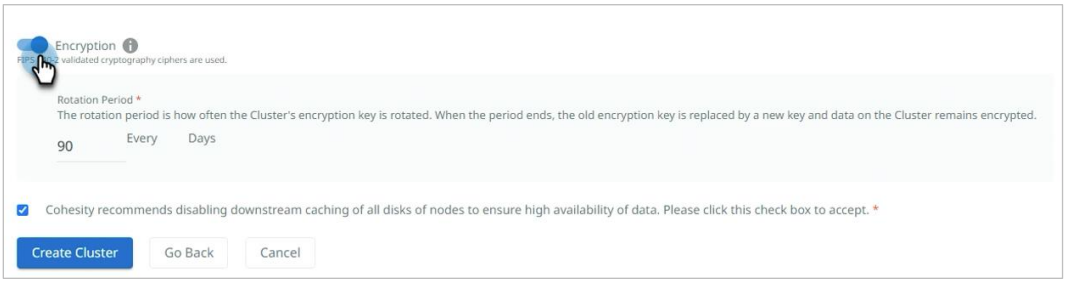
> **NOTE**: Cohesity does not support encryption based on TLS v1.1 or below.

Software Encryption

Cohesity clusters use AES-256 FIPS-approved algorithms, and the encryption keys are managed in an internal key management system (KMS), KMIP compliant KMS, or AWS KMS.

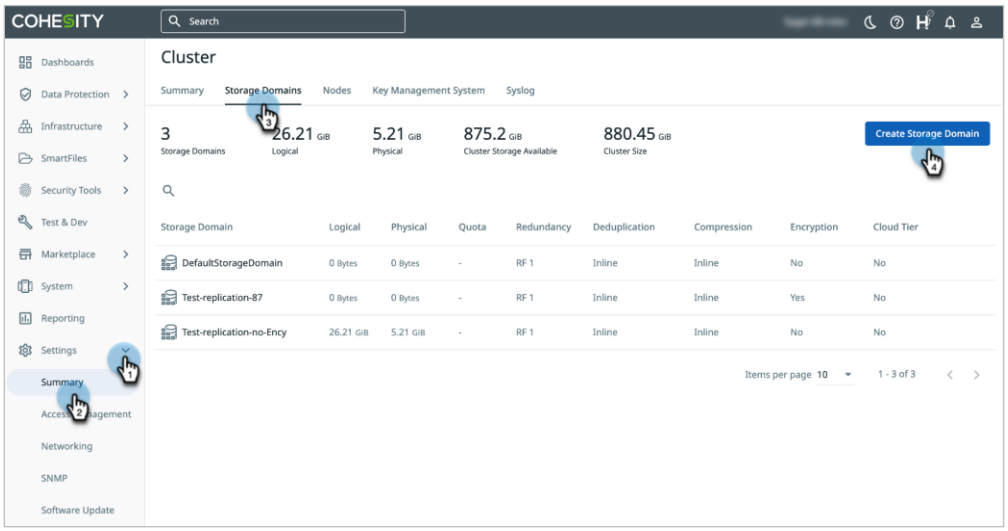
Cohesity highly recommends enabling cluster-wide encryption at initial installation. By default, the encryption key rotation period is set to 90 days. Change the default encryption key rotation period based on your organization's policy. If encryption is not enabled for a Cohesity cluster at the time of cluster creation, you can enable encryption at the Storage Domain level.

> **NOTE**: Cluster-Level Encryption is enabled by default when creating a new cluster from version 7.2.2 onwards. This cannot be disabled later. If you wish to out, then you must do it during cluster creation.

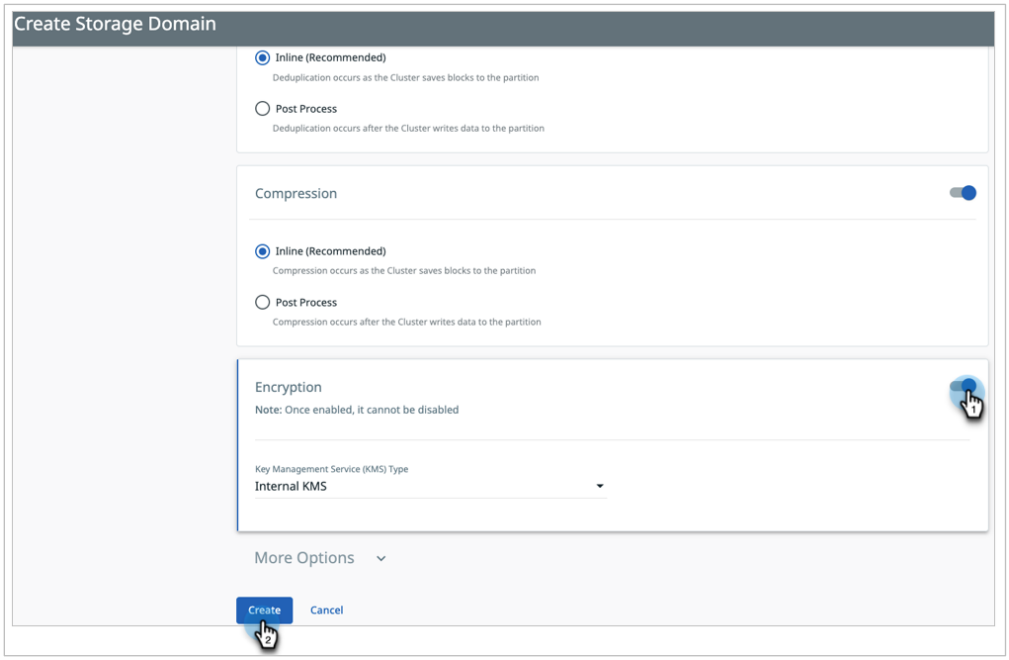


Enable Encryption at Storage Domain level

1. To enable encryption at the Storage Domain level, navigate to the Cohesity cluster and then go to **Settings** > **Summary** > **Storage Domains** > **Create Storage Domain**.



2. In the **Create Storage Domain**, enable **Encryption** and click **Create**.



> **NOTE**: You cannot disable the encryption once it is enabled at the cluster or Storage Domain levels.

For disaster recovery, you must establish replication between the primary (source) Cohesity cluster and target (remote) Cohesity cluster. Once you establish the connection, the primary Cohesity cluster transfers the captured IO Journals and the VMware snapshots to the secondary Cohesity cluster in encrypted form.

See Establish Replication Between the Cohesity clusters.

Node-to-Node Encryption

By encrypting the data before it is delivered to another node, node encryption helps to safeguard data in a network of connected Cohesity nodes. The data is decrypted once it reaches the right node.

Cohesity recommends enabling node-to-node encryption as an additional security measure.

NOTE: From Cluster version 7.1.1 onwards, node-to-node encryption is enabled by default. However, if you are upgrading your existing Cohesity clusters to version 7.1.1, you need to manually enable node-to-node encryption.

For more information, see Cohesity product documentation.

Use an External KMS

The Cohesity cluster supports AES-256 software encryption and has an internal Key Management Service (KMS) that automatically generates keys and stores them internally on the SSDs as encrypted keys. Alternatively, you can configure the cluster to store and manage your Key Encryption Keys (KEKs) on one of these external key management services. Configure your External KMS in High Availability mode for resilience purposes.

- Amazon Web Services (AWS) KMS.
- KMIP compliant KMS vendors such as Thales, Fortanix, Entrust, Vormetric DSM, HashiCorp, IBM SGKLM).

See Use an External KMS section in Cohesity documentation for more information.

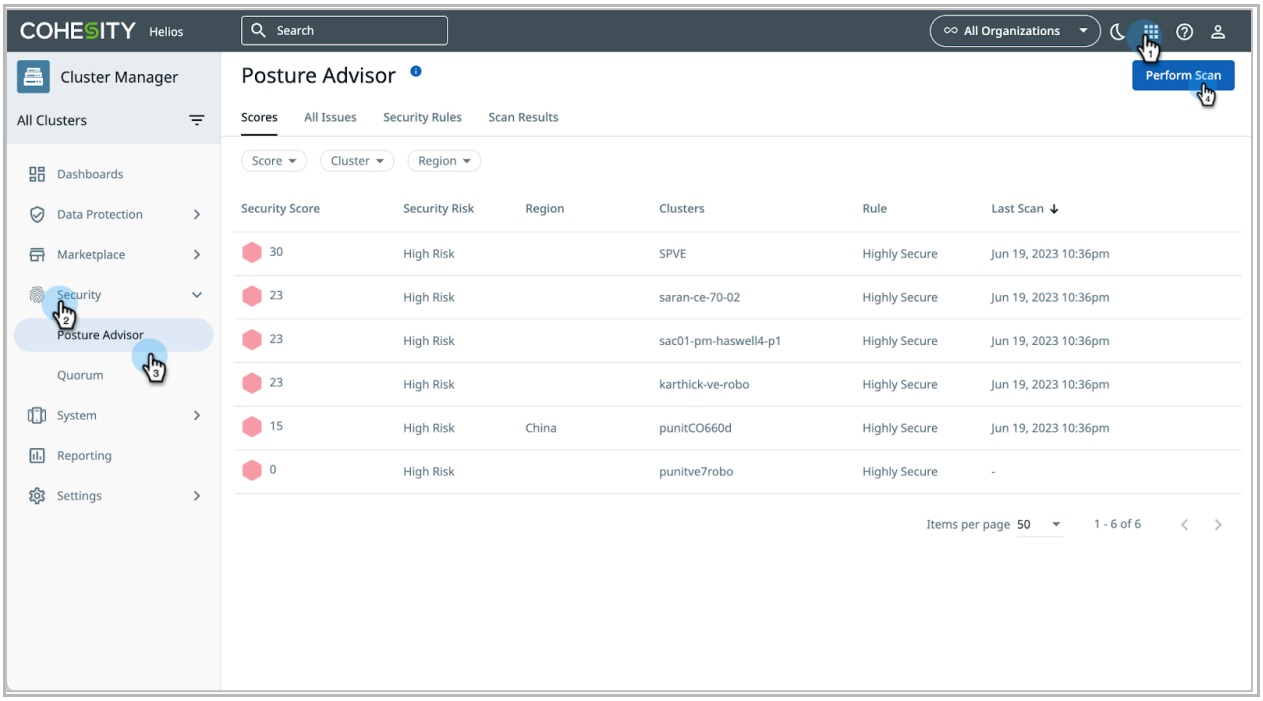
Continuous Security Monitoring

Now that you have completed the above security hardening tasks and implemented any other measures recommended or required by your own security practices/policies, you must continuously monitor, analyze your Cohesity cluster security posture, find deviations from best practices, and fix the security gaps.

Posture Advisor

The Cohesity Data Cloud platform offers Posture Advisor feature which enables you to view your Cohesity cluster security posture and provides actionable insights on your security configuration. To use this feature, you should first claim your cluster in Cohesity Helios.

To view the Security Dashboard from Cohesity Helios, navigate to the top-right icon  > **All Clusters** > **Security** > **Posture Advisor**.



- **Perform scans** frequently to view the security score of your clusters.
- **Inspect and remediate** clusters with security scores less than 90 (fix the high & medium risk) as a priority.
- **Inspect and remediate** all other identified issues.

For more detailed information on Cohesity Helios Posture Advisor, see Cohesity product documentation.

Security Alert Monitoring

Cohesity Data Cloud can fully integrate with external SIEM and log monitoring solutions by exporting platform logs in open format or through syslog server to third-party applications as SIEM for effective security alert monitoring.

System processes, user actions, and security events (Authentication Events) are logged. Logs are centrally managed through SIEM, which aggregates and correlates data from Cohesity Helios (customer-managed cluster, multi-cluster manager, and Helios Cloud) to generate alerts with Closed-Loop Ransomware Detection & Remediation integration with supported vendors such as Cisco XDR, Palo Alto Networks XSOAR, MS Sentinel, and CrowdSrtike Logscale.

Automate Incident Response (SOAR)

Cohesity Data Cloud can be integrated with an external Security Orchestration, Automation and Response (SOAR) platform to help customers carry out faster Incident response, improve Mean Time to Detect (MTTD) and Mean Time to Recover (MTTR) values, integrate data security events, and automate data recovery workflows into security incident response playbooks (which can accelerate recovery in the aftermath of a ransomware attack and bring efficiency to security and data operations). Cohesity has partnered with leading SIEM/SOAR technology vendors to effectively build in Apps available in the marketplace for integration, for example:

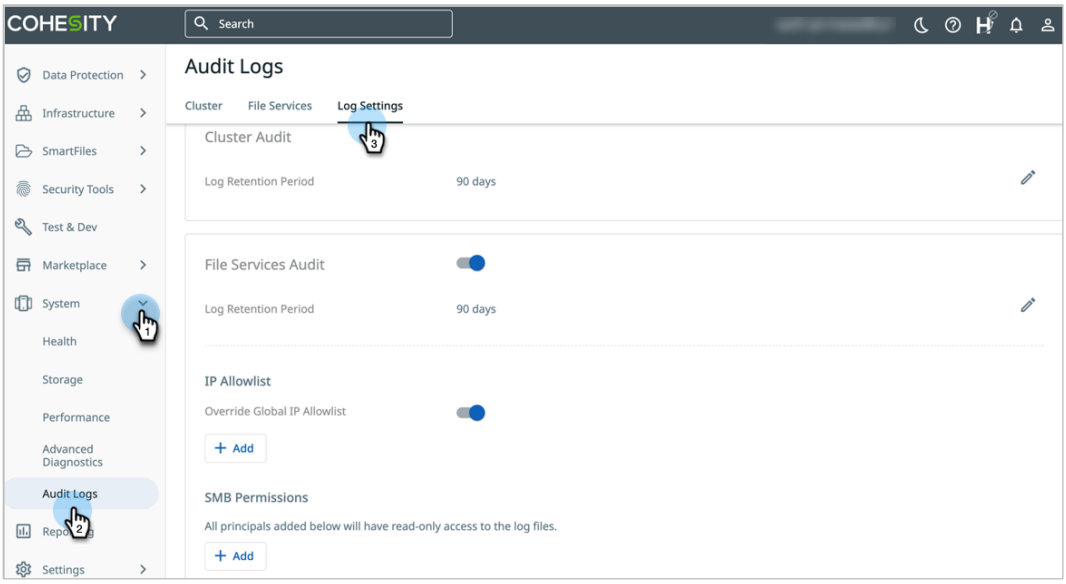
- Cisco XDR Integration
- Palo Alto Networks Cortex XSOAR Integration
- Microsoft Sentinel Platform
- Crowdstrike Falcon LogScale

Audit Logs

Audit logs help with security because they provide records of all the activities in the system. Audit logs provide monitoring data that you can use to analyze security breaches or vulnerabilities. Cohesity clusters generate cluster logs and file services logs.

- **Configure Audit Log Retention Period**—By default, the audit log retention period is set to 90 days. As per your organization's policy, you can choose to modify the retention period.
- **Enable Audit Log**—Cohesity recommends enabling the cluster and SmartFiles level audit logs to collect and review logs regularly.

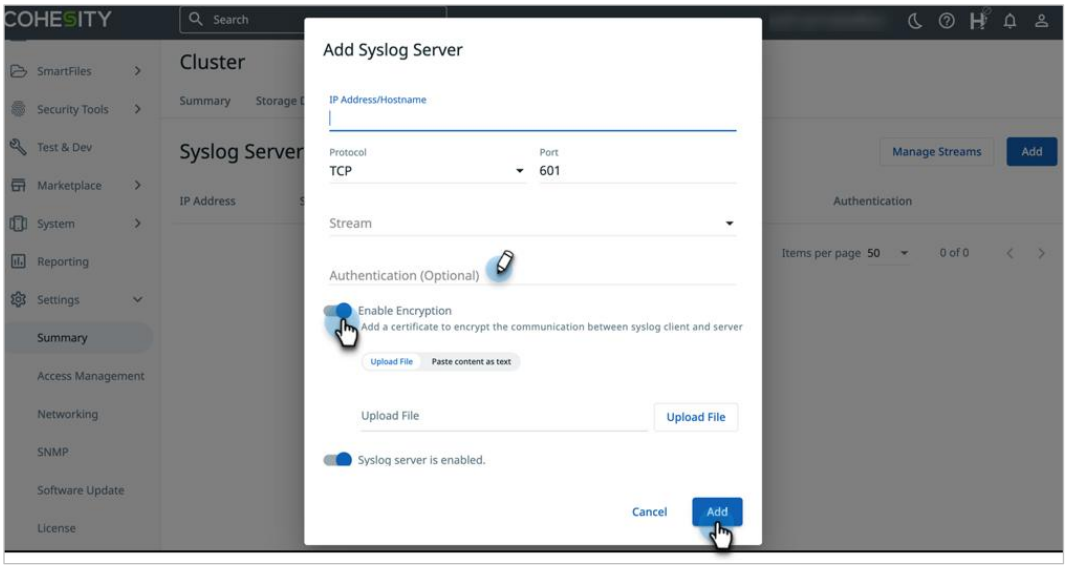
To view and configure the Cohesity cluster audit logs, navigate to **System** > **Audit Logs** > **Log Settings**.



Send Audit Logs to Syslog Server

Information stored in one location is often prone to accidental deletion. Offloading the application logs to the Syslog server assures log availability and integrity. Cohesity supports the configuration of a Syslog server for storing Cohesity audit logs.

- **Add a Syslog server** to send the Cohesity cluster audit logs to the syslog server.
- **Enable encryption** between the Cohesity cluster and the syslog server.
- **Configure the authentication** between the Cohesity cluster and the syslog server.



For more information, see Cohesity product documentation.

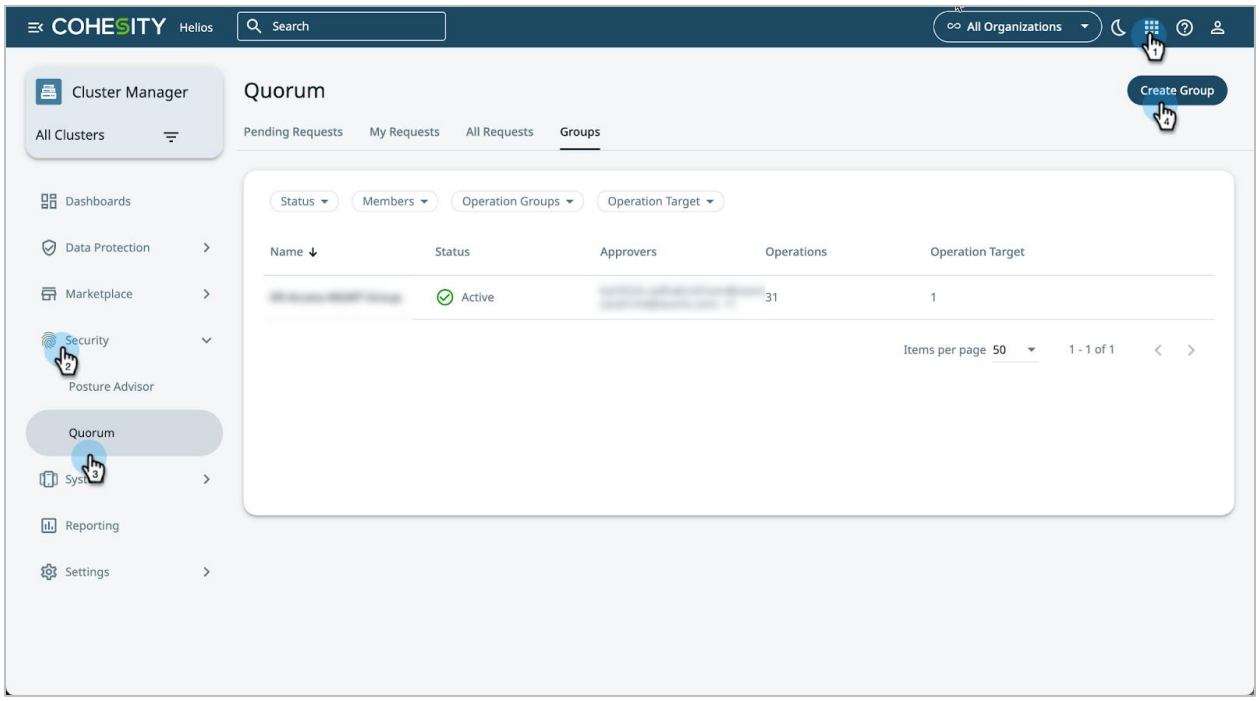
Configure Quorum Group

Data is the most valuable asset for any enterprise and like any precious asset, it is coveted, under attack and needs safeguarding. Significant amount of threat comes from insiders who have unrestricted access to data. Data Management from a Cohesity Data Cloud platform requires tight security controls and safety from enterprise data being compromised by a few reckless, malicious, or external attackers.

Cohesity Data Cloud has a unique feature called “Quorum Groups” to ensure sensitive or privileged operations must be approved by multiple people before those operations are executed. As soon as the requested operation reaches the approval threshold defined in the quorum group (within a defined time limit), the requested operation is executed immediately.

Cohesity recommends configuring sensitive data operations to require approval by a quorum group, which helps prevent the misuse of executing the privileges operations on the Cohesity Data Cloud without authorization.

Refer to product documentation to learn more about supported operations and best practices to use quorum in Helios.



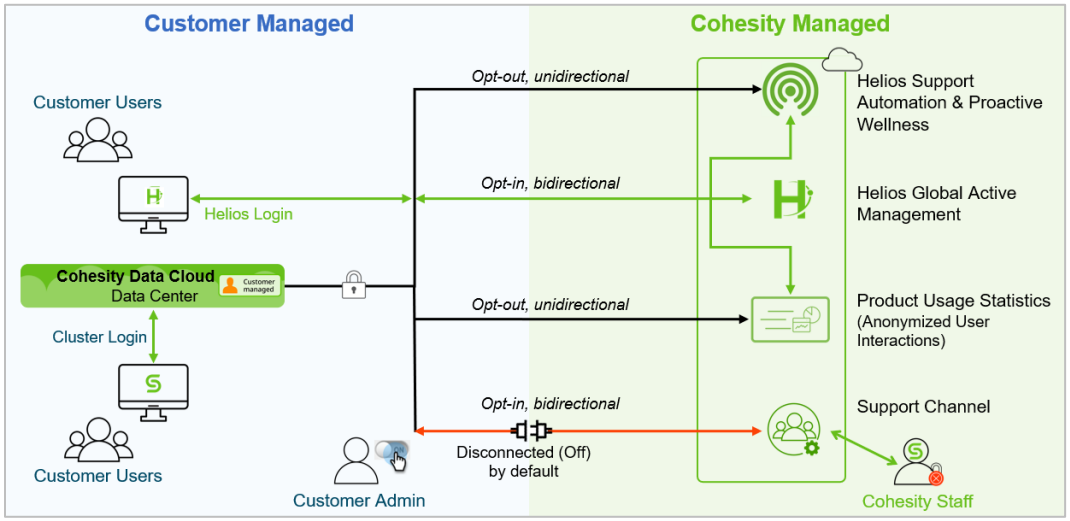
Manage Cluster Phone-Home Channels

Cohesity clusters have four 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.

NOTE: You, as a Cohesity customer, control each of these channels. You can enable or disable any or all of them. To do so or to learn more, see Cohesity Cluster Secure Phone-Home Security Brief.

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.

Figure 1: Cohesity Cluster Phone-Home Channels



- **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 for Remote troubleshooting** (*Opt-in*). Allows Cohesity technical experts to troubleshoot and remediate problems directly on your cluster. Cohesity recommends enabling the support channel temporarily only during troubleshooting periods

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, you can disable all the channels discussed here. To do so or to learn more, see Cohesity Cluster Secure Phone-Home Security Brief.

Appendix A: Cohesity Security Hardening Checklist

Table 3: Cohesity Security Hardening Checklist

NO.	SECURITY HARDENING CHECKLIST	MAINTENANCE PERIOD	WHEN TO PERFORM	COMPLETED
1	Upgrade Cohesity cluster to the latest LTS with the latest patches.	15 days	During cluster setup / Ongoing maintenance	
2	Secure passwords:			
	• Configure password policy—strength, lifetime, account lockout, and reuse.	90 days or as per organization's policy	During cluster setup / Ongoing maintenance	
	• Change default passwords for all local user accounts: ☐ Admin ☐ Support ☐ Cohesity_console (for non-DoD) ☐ IPMI ☐ Root (for DoD) ☐ Unique password for Primary and Replication clusters	One time	During cluster setup	
3	Secure account login with one or more methods as per below priority order: 1. Enable MFA for local user accounts. 2. Configure SAML SSO, enable MFA 3. Configure Active Directory, enable MFA for AD users, and join the Cohesity cluster to AD. 4. Rename the admin user account. (This workflow is available via CLI.)	90 days	During cluster setup / ongoing maintenance	
4	Secure BMC Access	One time	During cluster setup	
5	Create an automation user account with the least privileges (if required).	One time	During cluster setup	

NO.	SECURITY HARDENING CHECKLIST	MAINTENANCE PERIOD	WHEN TO PERFORM	COMPLETED
6	Assign least privileged roles to the users to perform operational tasks.	90 days	During cluster setup / ongoing maintenance	
7	Delete default self-signed certificates. Configure new self-signed or CA-signed certificates.	One time	During cluster setup	
8	Enable DataLock on protection policies applied to critical data.	90 days	During cluster setup / ongoing maintenance	
9	Secure Access Control:			
	• Configure Firewall profiles.	90 days	During cluster setup / ongoing maintenance	
	• Secure access for File and Object Services (IP allowlist).	90 days	During cluster setup	
	• Configure web session inactivity timeout and session limits.	One time	During cluster setup	
	• Enable login Banner as per organization's policy.	One time	During cluster setup	
	• Configure NTP with authentication.	One time	During cluster setup	
10	Enable encryption for data in rest and in transit; Use external KMS (recommended).	One time	During cluster setup	
11	Continuous Security Monitoring			
	• Posture Advisor—perform security scan; remediate high and medium risks.	15 days	Ongoing maintenance	
	• Configure centralized logs and auditing with external SIEM platforms.	One time	During cluster setup / ongoing maintenance	
	• SOAR integration to enable automation and fast Incident response.	One time	During cluster setup / ongoing maintenance	

NO.	SECURITY HARDENING CHECKLIST	MAINTENANCE PERIOD	WHEN TO PERFORM	COMPLETED
	• Enable File audit logs	One time	During cluster setup	
12	Configure Quorum Group	Ongoing	Ongoing operations	
13	Manage your Cohesity Cluster Secure Phone-Home channels.	Ongoing	During cluster setup / ongoing maintenance	
14	DoD mode controls (Applicable only for DoD customers)	Ongoing	During cluster setup / ongoing maintenance	
15	Ransomware attack protection and response readiness		Ongoing operations	

Appendix B: Terminology

Table 4: Terminology Used

TERM	DEFINITION
Cluster	A Cohesity cluster consists of three or more Cohesity nodes hosted either on hardware or on a virtual appliance.
Cohesity View	A Cohesity View provides a storage location with NFS, SMB, and S3 mount paths in a Storage Domain on the Cohesity cluster.
Data-at-Rest Encryption	Full at-rest encryption based on the strong AES-256 GCM/CBC (Cipher Block Chaining) standard on any storage medium.
Data-in-Transit Encryption	Encryption of data in transmission inside and outside of the Cohesity cluster.
DoD	Department of Defence
DoDIN APL	Department of Defense Information Network Approved Products List
Encryption	Process of converting plain text data into a secret code that conceals its true meaning.
KMS (Key Management System)	Create, manage, and regulate the use of cryptographic keys.
LTS (Long Term Support)	A stable release of Cohesity software is supported under the long-term support (LTS) policy of product lifecycle management for a longer period than the standard edition.
MFA (Multi Factor Authentication)	Authentication method that requires the user to provide 2 or more levels of verification to gain access to a Cohesity cluster.
NTP (Network Time Protocol)	An internet protocol used to synchronize cluster time with global NTP sources in a network.
Role-Based Access Control (RBAC)	Role is a collection of operations, such as creating a View or deleting a Protection Group. A role grants authorization to perform one or more operations.
SSO	Single Sign-On (SSO) is a session and user authentication service that permits a user to use one set of login credentials to access a Cohesity cluster.
SOAR	Security Orchestration, Automation, and Response refers to technologies that enable organizations to collect inputs monitored by the security operations team.
SIEM	Security Information and Event Management collects cluster logs in a centralized platform for detection, analytics, and response.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Karthick Radhakrishnan is the Director of the Security Center of Excellence, where he leads the development and management of Cohesity Security solutions and integrations.

Other essential contributors included:

- Patrick Ryan, Vice President, Assistant General Counsel
- Adaikkappan Arumugam, Director, Product Solutions

Document Version History

VERSION	DATE	DOCUMENT HISTORY
3.3	Mar 2026	• Content updates
3.2	Aug 2025	• Republished with latest template.
3.1	Apr 2025	• Removed the “Enable DoD Mode on Cohesity Cluster” section.
3.0	Jan 2025	• Added the “Securing BMC Access” section. • Added a row in Appendix A.
2.9	Nov 2024	• Updated the links to 7_1_2. • Replaced “SecureX” with “XDR”.
2.8	Sep 2024	• Minor update in the Appendix A section.
2.7	Aug 2024	• Content Updates.
2.6	Apr 2024	• Changing the terms from “Data-at-Transit” to “Data-in-Transit” and “data in flight” to “data in transit”.
2.5	Sep 2023	• Removed section “Hardware Encryption”
2.4	June 2023	• Added Quorum, SIEM/SOAR integrations
2.3	Mar 2023	• Added section "Enable DoD mode on Cohesity Cluster"
2.2	Oct 2022	• Added Section "Manage Cluster Secure Phone-Home Channels."

VERSION	DATE	DOCUMENT HISTORY
		• Remote section for support channel and folded it into "Manage Cluster Secure Phone-Home Channels." • Updated Appendix A Checklist to include Manage Cluster Secure Phone-Home Channels.
2.1	July 2022	• Security content revamp and latest LTS updates
2.0	Sep 2021	• 6.6 updates
1.4	Oct 2020	• 6.5.1b updates
1.3	July 2020	• Major update
1.2	Oct 2019	• Minor updates
1.1	Sep 2019	• Updated document
1.0	Mar 2019	• First full 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.