NetBackup Flex Appliance Getting Started and Administration Guide

Release 7.0

VERITAS
now part of Cohesity

NetBackup Flex Appliance Getting Started and Administration Guide

Last updated: 2026-08-28

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

Product overview

This chapter includes the following topics:

Introduction to Flex Appliance

Flex Appliance is a customizable data management solution that lets you consolidate multiple applications on a single hardware platform. With Flex Appliance, you can run concurrent instances of the following applications:

- NetBackup primary server
  You can also configure a BMR primary server with this application. However, the BMR boot server cannot be configured on the appliance.
- NetBackup media server with the following storage options:
  - Media Server Deduplication Pool (MSDP)
    You can also configure MSDP cloud storage with this application. Refer to the *NetBackup Deduplication Guide* after the instance is created.
  - AdvancedDisk
- NetBackup WORM storage

The NetBackup applications must follow the same compatibility requirements between NetBackup versions as any other NetBackup environment. See the *NetBackup Release Notes* for specifics.

For a full list of supported applications and versions for each Flex Appliance release, see the following article on the Support website:

Flex Appliance supported applications and usage information

Flex Appliance is currently available in English only.

This release is compatible with the following hardware:

- The 5372 Appliance, supporting all PCIe-based I/O configurations.

  Note: The 5372 Appliance supports 4-TB, 8-TB, and 20-TB disk drives. The 20-TB drive configuration is intended for long-term retention (LTR) workloads and supports a Media Server Deduplication Pool (MSDP) of up to 2.4 PiB. See the *NetBackup Deduplication Guide* for the MSDP capacity limits and the *Cohesity 5372 Appliance Product Description Guide* for the supported storage shelf configurations.

- The 5360 Appliance, supporting all PCIe-based I/O configurations.
- The 5350 Appliance, supporting all PCIe-based I/O configurations.
- The 5340 Appliance, supporting PCIe-based I/O configurations A, G, and H.
- An additional 53xx compute node for high availability (HA).

  Note: Both nodes must have the same PCIe-based I/O configuration.

- The 5270 Appliance, supporting all PCIe-based I/O configurations.
- The 5260 Appliance, supporting all PCIe-based I/O configurations.
- The 5250 Appliance, supporting all PCIe-based I/O configurations.
- The 5150 Appliance, supporting all PCIe-based I/O configurations.

See the *Product Description* guides for additional details about the appliance hardware and the available I/O configurations.

Flex Appliance terminology

Table 1-1 defines some of the common terminology used in Flex Appliance:

Table 1-1 Common terms

Term	Definition
Application	A software program that can be installed and used on a Flex appliance. For example, NetBackup.

Table 1-1 Common terms *(continued)*

Term	Definition
Instance	A single deployment of an application that was historically a standalone server. For example, a NetBackup primary server or a NetBackup media server.
Application add-on	A piece of software that can be installed on an application to modify or add to its capabilities. For example, a NetBackup Emergency Engineering Binary (EEB).
Repository	The location on the appliance that stores your applications, application add-ons, and Flex Appliance updates. You must add these files to the repository before you can use them.
Tenant	A separate space that you can create for a specific group of users and for a specific use. For example, you may create separate tenants for the different teams within your company.

About the Flex Appliance documentation

The following documents contain information about the Flex Appliance and application software:

- The *NetBackup Flex Appliance Getting Started and Administration Guide*
  Refer to this guide to configure and manage the Flex Appliance software, as well as for general information about creating and managing application instances.
- The *NetBackup Application Guides*
  Refer to these guides for more specific information about the NetBackup applications, including detailed instructions on how to create application instances of each supported version.

The following documents contain information about the appliance hardware:

- The *Hardware Installation Guide* for your particular model
- The *Product Description* for your particular model
- The *Appliance Safety and Maintenance Guide*

Flex Appliance also uses AutoSupport to monitor the appliance. You can find additional information about AutoSupport in the *Appliance AutoSupport Reference Guide*.

You can find the latest documentation on the Documentation page of the Support website. Navigate to the **Documentation** tab, then select **Flex Appliance OS** on the left-hand side.

API documentation is also available from the **Knowledge Base** page on SORT.

Chapter 2

Release notes

This chapter includes the following topics:

Flex Appliance 7.0 new features, enhancements, and changes

The following list describes the new features, enhancements, and changes in the Flex Appliance 7.0 release:

- You can configure multiperson authorization to add an extra layer of security by requiring additional authorized reviewers to approve critical operations.
  See “Managing multiperson authorization” on page 70.
- A new two-step update process has been introduced which allows parallel prechecks in multi-node clusters, reducing downtime and offering greater flexibility during updates.
  See “Updating Flex Appliance” on page 104.
- You can create custom roles with specific permission sets beyond the default options. This flexibility ensures that users have exactly the rights needed for their jobs, reducing unnecessary access and improving security.
  See “Creating custom roles” on page 50.

- You can restrict network access to services running inside application instances. By allowing access only through specified ports and an allowable IP/CIDR list, network access control minimizes attack exposure and ensures that only trusted sources can communicate with NetBackup instances.
  See “Network Access Control for application instances” on page 90.
- You can set resource limits to allocate CPU and memory resources efficiently to ensure optimal application performance.
  See “Setting resource limits” on page 89.
- Lockdown mode can be enabled at the appliance level using the Flex Appliance Console. At the instance level, you can change the lockdown mode.
  See “About lockdown mode” on page 125.
- You can retain the MAC address of the parent host interface across application stop and start events for an application instance.
  See “Preserving MAC address for application instances” on page 44.
- You can prevent service disruption caused by inode exhaustion by monitoring the inode usage for all application instance volumes.
  See “Inode usage monitoring and alerting” on page 139.
- After a new installation of Flex Appliance, the **Enforce multifactor authentication enforcement** dialog will appear at every login until the administrator explicitly enforces or opts out.
- The supported ciphers and message authentication codes (MACs) in the Flex Appliance Shell has been updated to improve overall system security.
  See “Accessing and using the Flex Appliance Shell” on page 29.
- The supported protocols and cipher suites for Flex Appliance Console access have been updated .
  See “Accessing and using the Flex Appliance Console” on page 31.
- The Flex Appliance Console has been enhanced to consistently use server time instead of client time, improving accuracy and consistency for all time-based operations across the interface.

Flex Appliance 7.1 new features, enhancements, and changes

The Flex Appliance 7.1 release includes a variety of fixes. It does not include any new features.

Supported update paths to this release

The following describes the supported update paths to Flex Appliance version 7.0:

- Direct update path
  You can update directly from version 3.2 or later to version 7.0.
- Multi-step update path
  Any appliance running an earlier version must first be updated to version 3.2. If you have a multi-node appliance, update both nodes to version 3.2 before you update to version 7.0.

Operational notes

This topic explains important aspects of Flex Appliance 7.0 operations that may not be documented elsewhere in the documentation.

The following list contains the notes and the known issues that apply for the Flex Appliance 7.0 software:

- After an abrupt power cycle, the Flex Appliance Console may display a “Bad Gateway” error.

  To fix this issue:

  - Log in to the Flex Appliance Shell.
  - Verify the container status using the **docker ps** command.
  - If the **peer-pod-peer** container is unhealthy, restart the **peer** service using the **systemctl restart peer** command.
  - Verify that the container is in a healthy state using the **docker ps** command.
  - Log in to the Flex Appliance Console.
- The AutoSupport notification UMI V-475-600-904 is delivered via SMTP and HTTP (SHI). If SNMP is the only configured AutoSupport delivery method, the notification will not be received, as SNMP delivery is not enabled for it.
- When a VLAN tag that is created on a physical network interface is deleted, the associated network configuration is removed successfully but the corresponding VLAN tag entry may continue to be displayed in the Flex Web Console UI. This occurs because Flex Appliance consolidates network interfaces from multiple sources, which can cause a stale VLAN entry to remain visible on the Console after deletion. This behavior is not observed when the VLAN tag is created on a bonded interface.
  Wait for up to 15 minutes and refresh the Flex Appliance Console. The stale VLAN tag entry will be automatically removed.

- When the appliance turns on, you may receive the following false alerts if the services take longer than usual to start:
  V-475-130-30007: The metrics-node service is not in an optimal state.
  V-475-130-30009: The metrics-storage service is not in an optimal state.
  If you have not received a second alert after four hours, you can safely ignore these alerts.
- If you have more than 10 VLAN tags configured with an IPv6 network, instances may not start cleanly. To avoid this issue, do not configure more than 10 VLAN tags with an IPv6 network.
- Flex Appliance does not currently restrict you from adding a local user and a remote user with the same username. However, upgrade issues can occur if you do. Do not use duplicate usernames across local and remote users.
- If a server communicates with the appliance with a domain name that is not in the appliance `hosts` file, the server name is not masked in the logs.
- If you generate a Data Collect log package with data masking enabled, the `private_map` file that is included uses the same key value for multiple entries.
- Alerts are not currently sent for the metrics that can be set with the `set alerts hardware-threshold` command.
- During a firmware update, an issue can occur with the storage shelf controller that causes an update failure message to appear. If you see a failure message, it may have appeared in error, and the update may still have worked. Run the following command to confirm the firmware version:
  `show hardware-health primaryshelf component=controller`
- When you install application add-ons on an instance, the Flex Appliance Console lets you select different versions of the same OST plug-in. However, this configuration is not supported, and if you select more than one version of the same plug-in, the **Install add-ons** page shows duplicate entries. Only install one version of each OST plug-in on an instance. If you need to change the version of an OST plug-in that is already installed, first uninstall it, and then install the new version.

Flex Appliance 7.0 Fixed issues

The following list contains the known issues that were fixed and that are now included in this release of Flex Appliance:

- Tooltip text for partial storage rekey on System topology page was incorrect.
- Rollback operations failed with the error:

```
Ansible requires the locale encoding to be UTF-8; Detected ISO8859-1.
```

- Sync-settings operations failed when AutoSupport was not running.
- `settings-sync.service` was found in a failed state after a successful SURE v34 upgrade.
- The Tab key did not work for `set date ntp` command.
- An incorrect MAC address was stored for a slave interface in the etcd key `/cluster/nodes/specs/<node>/network-cards`.
- Assigning two VLANs to a media instance failed when the interface IP matched the gateway due to missing UI validation.
- The `Shelf Order` command description displayed an incorrect message after running `support show-shelf-order` command.
- The `Create Replica` operation on Site B failed on the UI with an internal server error (V-492-100-505).
- After a SURE v34 run on the second node, the first node sent an SMTP alert for remote management with status Abnormal.
- After a SURE v34 upgrade, SMTP alerts were sent for application instances with status:

  ```
  Application instance <instance_ID> OFFLINE
  ```

- SAR logs were not collected using `support data-collect performance at=now` command.
- The `DELETE /api/v1/nodes/{hostname}/logs API` returned a non-JSON response for certain special characters.
- The upgrade from Flex Appliance version 4.0.2 to 6.0 failed.

Flex Appliance 7.1 release content

This release includes fixes for customer-reported defects and security vulnerabilities. See the *Release Notes* PDF on the Downloads page for more information.

Chapter 3

Getting started

This chapter includes the following topics:

Initial configuration guidelines and checklist

Review the following information before you perform the initial configuration on a new Flex appliance:

Table 3-1 Flex Appliance configuration guidelines and checklist

Parameter	Description
Network cabling for the 53xx appliance	The following 53xx appliance ports must be connected to the network for initial configuration: ■ The remote management (IPMI) port Used to connect to the Veritas Remote Management Interface. **Note:** The remote management port must be configured before you begin initial configuration. If it is not configured, do one of the following: For a 5350, 5360 or 5372 appliance, refer to the *Hardware Installation* guides for the procedure. For a 5340 appliance, contact Technical Support and ask your representative to reference article 100042482. ■ host1 or host0 Used to connect to the Flex Appliance Console. Cohesity recommends that you connect both host1 and host0 for maximum resiliency, but only one of them is required. **Note:** These ports are labeled ETH0 and ETH1 on the 53xx nodes. ■ privnic1 and privnic0 (multi-node appliances only) Used for communication between nodes. **Note:** These ports are labeled ETH2 and ETH3 on the 53xx nodes. ■ Four to eight 25-10Gb Ethernet ports per node on the 5372 Four to eight 25-10Gb Ethernet ports per node on the 5360 Two to eight 25-10Gb Ethernet ports per node on the 5350 Two to ten 10Gb Ethernet ports per node on the 5340 Used for the application instances. See the *Hardware Installation* or the *Product Description* guides for more details.
Network cabling for the 52xx appliance	The following 52xx appliance ports must be connected to the network for initial configuration: ■ The remote management (IPMI) port Used to connect to the Veritas Remote Management Interface. **Note:** The remote management port must be configured before you begin initial configuration. If it is not configured, refer to the *Hardware Installation* guides for the procedure. ■ host0 host1 (only for 5270 appliance) Used to connect to the Flex Appliance Console. ■ Two to eight 25-10Gb Ethernet ports on the 5270 Two to six 25-10Gb Ethernet ports on the 5260 Two to six 25-10Gb Ethernet ports on the 5250 Used for the application instances. See the *Hardware Installation* or the *Product Description* guides for more details.

Table 3-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description
Network cabling for the 5150 appliance	The following 5150 appliance ports must be connected to the network for initial configuration: ■ The remote management (IPMI) port Used to connect to the Veritas Remote Management Interface. **Note:** The remote management port must be configured before you begin initial configuration. If it is not configured, refer to the *5150 Appliance Hardware Installation Guide* for the procedure. ■ host0 Used to connect to the Flex Appliance Console. ■ Two 25-10Gb Ethernet ports, two 10GBASE-T Ethernet ports, or four 1GBASE-T Ethernet ports, depending on the purchase configuration Used for the application instances. See the *5150 Appliance Hardware Installation Guide* or the *5150 Appliance Product Description* for more details.
Connectivity during initial configuration	When you perform the appliance initial configuration, you must take precautions to avoid loss of connectivity. Any loss of connectivity during initial configuration results in failure. The computer that you use to configure the appliance should be set up to avoid the following events: ■ Conditions that cause the computer to go to sleep ■ Conditions that cause the computer to turn off or to lose power ■ Conditions that cause the computer to lose its network connection

Table 3-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description

Required names and addresses	Before the configuration, gather the following information:
	■ (53xx appliance only) IP address for the Flex Appliance Console
	■ (53xx appliance only) Hostname for the Flex Appliance Console
	The Fully Qualified Domain Name (FQDN) can be a maximum of 45 characters.
	Note: On 53xx appliances, the Flex Appliance Console IP address/hostname must be unique and must not match the IP address/hostname of any node configured using the `setup configure-network` command.
	■ IP address for each node in the appliance
	■ Hostname for each node in the appliance
	The Fully Qualified Domain Name (FQDN) can be a maximum of 45 characters.
	■ Default gateway
	■ (Optional) DNS server IP address
	■ DNS domain
	■ (Optional) Search domain
	Note: You can use IPv4 or IPv6 addresses for the appliance, but a dual-stack network is not supported. The IPv4 and IPv6 protocols are disabled until you complete the initial configuration. After configuration, the protocol that you did not configure remains disabled.
	The following subnets are also reserved for internal use and cannot be used for the appliance network:
	192.168.227.0/24 and fdf8:192:168:227::/120
	192.168.228.0/24 and fdf8:192:168:228::/120
	192.168.229.0/24 and fdf8:192:168:229::/120
	192.168.230.0/24 and fdf8:192:168:230::/120
	If you plan to use DNS, make sure that forward and reverse DNS lookups are configured properly in your environment. If a forward or a reverse DNS lookup returns multiple records, the initial configuration may fail. You can check the DNS configuration with the following commands for each node. Each command should return only one entry.
	Linux:
	`dig +short @<DNS server IP address> a <node FQDN>`
	`dig +short @<DNS server IP address> -x <node IP address>`
	Windows:
	`nslookup <node IP address>`
	`nslookup <node hostname>`

Table 3-1 Flex Appliance configuration guidelines and checklist *(continued)*

Parameter	Description
Default username and password	New appliances are shipped with the following default login credentials: ■ Username: **hostadmin** ■ Password: **P@ssw0rd**
Firewall port usage	Make sure that the following ports are open if a firewall exists between the appliance and the network: ■ 22 (SSH) must be allowed to each node. ■ 443 (HTTPS) must be allowed to the Flex Appliance Console.

Performing the initial configuration

The following procedure explains how to configure the Flex Appliance software on a new appliance.

Note: If more than the tested number of Fibre Channel devices or paths are connected to the appliance, Cohesity recommends that you disable the ports or disconnect the devices before you begin this procedure. When the procedure is complete, reenable or reconnect them. You may need to scan the ports from the Fibre Channel interfaces page.

See "Managing the appliance Fibre Channel ports" on page 41.

To configure Flex Appliance

1. Review the initial configuration guidelines and checklist to make sure that you have all of the necessary information to complete this procedure.

   See "Initial configuration guidelines and checklist" on page 18.

2. Use the following steps to access the Flex Appliance Shell from the Veritas Remote Management Interface:

   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 139 or later recommended (minimum version 105 or later)
     - Mozilla Firefox version 142 or later recommended (minimum version 140 or later)

- Enter the IP address that is assigned to the remote management (IPMI) port of the appliance node. If you have a multi-node appliance, select one of the nodes to use to begin the initial configuration.
- Log in to the Veritas Remote Management Interface with the following default credentials:
  - **Username**: **sysadmin**
  - **Password**: **P@ssw0rd**
- Change the **sysadmin** password from the known default password as follows:
  - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
  - Click **Modify User**.
  - Select the **Change Password** check box and enter a new password.
- Do one of the following to launch the Flex Appliance Shell:
  - Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
  - If available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**.

Note: Availability of the HTML5 option depends on the appliance firmware version. You can check the version from the **System** > **System Information** page. The BIOS ID must show version 00.01.0016 or later.

---

3 Log in to the Flex Appliance Shell with the following default credentials:

- Username: **hostadmin**
- Password: **P@ssw0rd**

See "Accessing and using the Flex Appliance Shell" on page 29.

4 Enter the following command to change the password for the **hostadmin** user:

```
set user password
```

5 Enter the following command to configure the host network:

```
setup configure-network
```

Follow the prompts to enter the host network information. You can enter multiple DNS server IP addresses or search domains using a comma-separated list. You can enter up to three DNS server IP addresses. If you need to add more, you can use the `set network dns` command after initial configuration.

6 If you did not fill in the optional DNS parameters or want to bypass DNS for specific hosts, you must add the hostname resolution information to the appliance `Hosts` file. Use the following steps:

- Enter the following command:

  ```
  system add-host
  ```

- One at a time, enter the required hostname information for the following:
  - The node
  - The Flex Appliance Console if the `setup configure-network` prompts asked for it

  You can also add the information for the other node if you have a multi-node appliance, as well as any instances you plan to create, or you can add that information later.

7 Use the `set date` commands to set the date and time. See "Setting the date and time for appliance nodes" on page 35.

8 Enter the following command to configure the Flex Appliance Console:

```
setup configure-console
```

Follow the prompts as applicable to your appliance to enter the console network information.

Note: Depending on the number of storage shelves you have in the appliance, this step may take up to 15 minutes to complete. When it is complete, the shell refreshes with new command options.

---

9 If you have a single-node appliance, the initial configuration process is now complete. Proceed to the next steps that are listed at the end of this topic.

If you have a multi-node appliance, add the second node. Then proceed to the next steps that are listed at the end of this topic.

See "Adding a node" on page 25.

Note: If any part of the initial configuration fails, refer to the error message to resolve the issue and try again. If you resolve the error but experience the same failure, perform a factory reset and a storage reset to return the appliance to its factory configuration. Then restart the initial configuration process.

See "Performing a factory reset" on page 159.

See "Performing a storage reset" on page 170.

Next steps

After you have completed the initial configuration, you must perform the following tasks before you can create an application instance and start using Flex Appliance:

- Verify that you can access the Flex Appliance Console.
  See “Accessing and using the Flex Appliance Console” on page 31.
- Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
  See “Configuring or editing a network interface” on page 40.
  See “Creating a network bond” on page 37.
- Add the applications that you want to use to the repository.
  See “Managing the repository” on page 80.
- Add at least one tenant.
  See “Adding a tenant” on page 47.
- Cohesity recommends that you change the BIOS password.
  See “Changing the BIOS password” on page 110.
- Cohesity also recommends that you register your appliance to ensure that you receive maximum support in the event of a failure. Registration helps Cohesity to contact the right person and to dispatch field services to the correct location for repairs.
  See “Registering an appliance” on page 133.

Once all of these tasks have been completed, you are ready to create an instance and start using Flex Appliance.

Adding a node

Flex Appliance supports up to two nodes on the 53xx appliance. You can add a second node during initial configuration or any time after.

A multi-node appliance provides the following benefits:

- Increased efficiency with a shared workload
- Automatic failover for a single-node failure

Adding a second node consists of the following tasks:

- Perform the host network configuration on the new node.
- From the existing node, add the new node to the appliance.

Note: If you add a node to an appliance that has already been configured and is in lockdown mode, the same lockdown mode is automatically enabled on the new node. However, if you are configuring a new multi-node appliance, you must configure all nodes before you enable lockdown mode.

Tasks for adding a node

To perform the host network configuration on the new node

1. Verify the version compatibility between the new node and the node that you want to add it to. The nodes must be running the same version of Flex Appliance, but they can have different security patches installed.

   If the existing node is at a lower version that does not meet these requirements, update that node before you add the new one. If the new node is at a lower version that does not meet these requirements, it must be reimaged to the later version.

2. Gather the following details for the new node that you want to add to the appliance:

   - IP address
   - Hostname

   Note: The following subnets are reserved for internal use and cannot be used for the appliance network:

   192.168.227.0/24 and fdf8:192:168:227::/120

   192.168.228.0/24 and fdf8:192:168:228::/120

   192.168.229.0/24 and fdf8:192:168:229::/120

   192.168.230.0/24 and fdf8:192:168:230::/120

   Gather the following details from the appliance that you want to add the node to:

   - Default gateway
   - (Optional) DNS server IP address
   - DNS domain
   - (Optional) Search domain

3. If the node that you want to add has Fibre Channel connections to external devices, disable all Fibre Channel ports that are connected to those devices. You do not need to disable the ports that are connected to the appliance storage shelves.
4. Use the following steps to access the Flex Appliance Shell from the Veritas Remote Management Interface:
   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 139 or later recommended (minimum version 105 or later)
     - Mozilla Firefox version 142 or later recommended (minimum version 140 or later)
   - Enter the IP address that is assigned to the remote management port of the new node.
   - Log in to the Cohesity Remote Management Interface with the following default credentials:
     - **Username**: **sysadmin**
     - **Password**: **P@ssw0rd**
   - Change the **sysadmin** password from the known default password as follows:
     - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
     - Click **Modify User**.
     - Select the **Change Password** check box and enter a new password.
   - Navigate to **Remote Control** > **Console Redirection** and click **Launch Console** to launch the Flex Appliance Shell.
5. Log in to the Flex Appliance Shell with the following default credentials:
   - Username: **hostadmin**
   - Password: **P@ssw0rd**
6. Enter the following command to change the password for the **hostadmin** user:

   ```
   set user password
   ```

7 Enter the following command to configure the host network:

```
setup configure-network
```

Follow the prompts to enter the host network information. You can enter multiple DNS server IP addresses or search domains using a comma-separated list.

8 If you did not fill in the optional DNS parameters or want to bypass DNS for the new node, you must add the hostname resolution information for the new node to the appliance `Hosts` file. If you did not already add this information when you configured the first node, enter the following command:

```
system add-host
```

Follow the prompts to enter the required information for the new node.

9 Use the `set date` commands to set the date and time. Make sure that the settings are in sync with the other node. See “Setting the date and time for appliance nodes” on page 35.

To add the new node to the appliance

1 Log in to Flex Appliance Shell from the other, preexisting node that was previously configured for the appliance.

2 From the preexisting node, enter the following command to add the new node to the appliance:

```
setup add-node
```

Follow the prompts to add the node. When you are prompted for the new node's password, enter the **hostadmin** password that you set in the previous procedure.

Note: Do not perform any other tasks on the appliance until the `add-node` operation is complete.

---

3 When the `add-node` operation is complete, exit the Flex Appliance Shell from the new node that you just added to the appliance. Then launch a new session from the Veritas Remote Management Interface or open an SSH session to the node. The shell should now display additional command options.

4 If the node that you added has existing Fibre Channel connections, enable them and then run the following command:

```
system sync-settings
```

Alternatively, you can first clean and then scan the ports from the Flex Appliance Console. See "Viewing the devices that are connected to the Fibre Channel ports" on page 43.

5 If you added this node as part of the appliance initial configuration, return to the initial configuration procedure and refer to the next steps at the end of the procedure to get started using the appliance.

See "Performing the initial configuration" on page 22.

Accessing and using the Flex Appliance Shell

You can use the Flex Appliance Shell to perform the initial configuration, monitor the appliance hardware, and manage some of the settings.

Accessing the Flex Appliance Shell

To access the Flex Appliance Shell for most operations, open an SSH session to the appliance node and log in with the username **hostadmin** and the password that you set during initial configuration.

Note: If you have a multi-node appliance, you must log in to each node individually.

If you have not completed the initial configuration yet, you can access the shell through the Veritas Remote Management Interface. Refer to the initial configuration procedure for instructions.

Cohesity recommends that you also log in through the remote management interface for the following operations:

- Restarting the node
- Factory resets
- Reimaging

Note: When you access the Flex Appliance Shell through the Veritas Remote Management Interface, do not enter **alt+PrtScn** while a command is running. If you do, the command fails, and it still may not work when you try to rerun it.

To conform with the Federal Information Processing Standards (FIPS) and the Security Technical Implementation Guide (STIG), the Flex Appliance Shell supports only the following ciphers and message authentication codes (MACs):

- Ciphers:
  - aes256-gcm@openssh.com
  - aes256-ctr
- MACs:
  - hmac-sha2-512-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512
  - hmac-sha2-256

Older SSH clients are likely to prevent access to the appliance. Check to make sure that your SSH client supports the listed ciphers and MACs, and update to the latest version if necessary. Default SSH client settings may not be FIPS- and STIG-compliant, which means you may need to select them manually in your SSH client configuration.

Navigating the Flex Appliance Shell

Note: When you log in for the first time, the available commands are limited to those that you can run on an unconfigured appliance. Complete the initial configuration to gain access to the rest of the command options. See "Performing the initial configuration" on page 22.

The Flex Appliance Shell includes the following command views:

- `setup`
  Includes all of the commands for initial configuration.
- `system`
  Includes the commands you can use to manage the appliance OS, system services, and hosts file settings.
- `show`
  Includes the commands you can use to show the current appliance settings and information about the appliance hardware.
- `set`
  Includes the commands you can use to modify the appliance settings.
- `support`

Includes the commands you can use to access privileged operations and manage storage shelves. This view is primarily intended for Technical Support.

- Also includes the `support shell`, which has a command prompt to let you view read-only information on the appliance, including performance metrics.

The following is a list of tips on how to use the Flex Appliance Shell:

- You can press the **?** key at any time to display more information about the commands or sub-views. If you press **?** after you enter a command, the format and usage of the parameters for that command is displayed.
- To type a **?** without displaying the help, first press **Ctrl** + **v**.
- You can press **Alt** + **s** at any time to view a list of shell shortcuts and additional features.
- The Flex Appliance Shell works similarly to the Bourne-Again Shell (BASH) and supports all of the same keyboard shortcuts.
- Additional Linux commands are available by typing the full path to the command. For example: `/usr/bin/top`.

  The available commands are dependent on the security permission settings of the user.
- In the documentation, command variables are italicized or in angular brackets (<>). Replace these variables with the appropriate information for each command.

See "Common tasks in Flex Appliance" on page 36.

Accessing and using the Flex Appliance Console

After you have configured Flex Appliance, you can sign in to the Flex Appliance Console to use and manage the appliance software.

Accessing the Flex Appliance Console

To access the Flex Appliance Console

1. Open a web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
   - Google Chrome version 139 or later recommended (minimum version 105 or later)
   - Mozilla Firefox version 142 or later recommended (minimum version 140 or later)

Note: These browsers may display a **Privacy error** or **Insecure Connection** page when you access the Flex Appliance Console. Use the **Advanced** option on the page to proceed.

2 Navigate to **https://*console.domain***, where *console.domain* is one of the following:

- If you have a 52xx or a 5150 appliance, *console.domain* is the fully qualified domain name (FQDN) or the IP address that you entered during initial configuration.
- If you have a 53xx appliance, *console.domain* is the fully qualified domain name (FQDN) or the IP address that you entered for the Flex Appliance Console during initial configuration.

3 When you sign in for the first time, use the following default credentials:

- **Username**: **admin**
- **Password**: **P@ssw0rd**

After you have signed in, you are required to add a local user and are then signed out. Use the new local user's credentials to sign in again.

Navigating the Flex Appliance Console

To navigate the Flex Appliance Console, use the icons in the left-side navigation bar or the **Settings** drop-down menu in the upper-right corner. To see the page names in the navigation bar, hover over the icons or use the **>>** icon at the top to expand the entire bar.

The Flex Appliance Console includes the following pages:

Home

The home page includes various widgets that provide information about the status of the appliance. To return to the home page at any time, click the **Home** icon in the left-side navigation bar.

System topology

The **System topology** page shows a complete overview of the appliance nodes, storage, and instances. To access this page, click the **System topology** box on the home page or click the **System topology** icon in the left-side navigation bar.

Note: The **System topology** page shows the full capacity of the appliance storage. However, not all of the storage is available for use. You can see the usable storage capacity when you create or resize an instance.

Activity Monitor

The **Activity Monitor** page shows the tasks that have been performed on the Flex Appliance Console and their current status. To access this page, click the **Activity Monitor** icon in the left-side navigation bar.

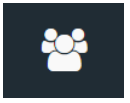
Repository

The **Repository** page lets you manage the applications, application add-ons, and update packages for Flex Appliance. To access this page, click the **Repository** icon in the left-side navigation bar.

Tenants

The **Tenants** page lets you manage tenants. To access this page, click the **Tenants** icon in the left-side navigation bar.

Access management



The **Access management** page lets you manage users for the Flex Appliance Console. To access this page, click the **Access management** icon in the left-side navigation bar.

Network interfaces

The **Network interfaces** page lets you view and configure the appliance's network interfaces. To access this page, click the **Network interfaces** icon in the left-side navigation bar.

Fibre Channel interfaces

The **Fibre Channel interfaces** page lets you check the status of the appliance Fibre Channel ports and view the devices that are connected to them. To access this page, click the **Fibre Channel interfaces** icon in the left-side navigation bar.

Remote replication

The **Remote replication** page lets you configure and manage remote replication with a paired appliance. To access this page, click the **Remote replication** icon in the left-side navigation bar.

Settings

The **Settings** pages let you manage the settings for security and compliance, alert configuration, and remote management. To access these pages, click the gear icon in the upper-right corner of the page.

See “Common tasks in Flex Appliance” on page 36.

For Flex Appliance Console access, the following protocols and ciphers are supported:

- TLSv1.3
  - TLS_AES_256_GCM_SHA384
- TLSV1.2
  - ECDHE-RSA-AES256-GCM-SHA384
  - DHE-RSA-AES256-GCM-SHA384

Setting the date and time for appliance nodes

Follow these steps to set the date and time on the appliance nodes.

Note: The Network Time Protocol (NTP) is required for multifactor authentication.

To set the date and time using NTP

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set date ntp
   ```

2. Press **Enter**.
3. Follow the prompts to set the NTP server.
4. If you have a multi-node appliance, repeat this procedure on the other node.

To set the date and time by entering the date and time manually

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set date manual-date
   ```

2. Press **Enter**.
3. Type the date and time, and then press **Enter**.
4. If you have a multi-node appliance, repeat this procedure on the other node.

To set the time zone

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set date timezone
   ```

2. Press **Enter**.
3. Type the number that corresponds to your continent or ocean, and then press **Enter**.
4. Type the number that corresponds to your country, and then press **Enter**.
5. Type the number that corresponds to your time zone, and then press **Enter**.

6 Type **1** to verify that the time zone is correct, and then press **Enter**.

7 If you have a multi-node appliance, repeat this procedure on the other node.

Common tasks in Flex Appliance

The following table contains quick links on how to perform common tasks in Flex Appliance.

Table 3-2

Task	Quick links
Configuring Flex Appliance	See "Performing the initial configuration" on page 22. See "Adding a node" on page 25.
Managing tenants and users	See "Managing Flex Appliance Console users and tenants" on page 46.
Modifying settings	See "Configuring or editing a network interface" on page 40. See "Creating a network bond" on page 37. See "Setting the date and time for appliance nodes" on page 35.
Configuring Call Home	See "About AutoSupport and Call Home" on page 134.
Monitoring the appliance	See "Viewing the hardware status" on page 141. See "Viewing hardware faults" on page 145. See "Viewing system data" on page 145.
Adding files to the repository	See "Managing the repository" on page 80.
Creating instances	See "Creating application instances" on page 83. See "Managing application instances from Flex Appliance" on page 85.

Chapter 4

Managing network settings for instances

This chapter includes the following topics:

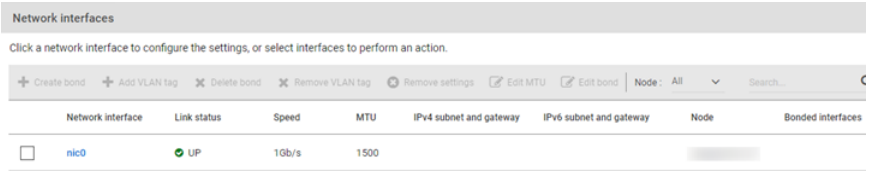
Creating a network bond

If you have more than one node, you must create a network bond on each appliance node after all of the nodes are added. Use the same network interfaces and bonding mode for the bond on each node.

To create a network bond

1. On the Flex Appliance Console, click the **Network interfaces** icon in the left-side navigation bar to open the **Network interfaces** page.

   It may take a few minutes to load.



2. Select the check box next to the name of each network interface that you want to include in the bond, then click **Create bond**.
3. Enter a unique bond name and select the bond mode.

   The following bond modes are available:

   - 802.3ad (LACP) - this is the default bond mode value

     Note: If you select this bond mode, all of the network interfaces in the bond must be on the same port channel. If they are not, the bond speed is less than the sum of the interface speeds. If the bond speed is not as expected after you create the bond, run the following command in the Flex Appliance support shell:

     `/bin/grep "Aggregator ID" /proc/net/bonding/<bond name>`

     The Aggregator IDs should all be the same. If they are not, run the following command and check the Aggregator ID of each interface to determine which one is on a different port channel:

     `/bin/cat /proc/net/bonding/<bond name>`

   - balance-rr
   - active-backup
   - balance-xor
   - broadcast
4. Click **Create**.
5. Configure the new bond.

   See “Configuring or editing a network interface” on page 40.

Editing a network bond

Follow these steps to edit a network bond to change the bonded interfaces.

To edit a network bond

1. From the **System topology** page on the Flex Appliance Console, click on each of your application instances and verify that the bond is not listed in the **IP address and interface pairs** field. If the bond is listed for one or more instances, edit the network of each instance to remove the bond. See "Editing instance network settings" on page 87.

   You may need to add a different IP address and interface pair if the bond that you want to edit is the only interface that is assigned to the instance. If you do not have another available configured interface, configure an interface with placeholder values that you can use until you complete the edits. See "Configuring or editing a network interface" on page 40.

2. Navigate to the **Network interfaces** page and select the bond that you want to edit.
3. Click **Edit bond**.
4. Make the required changes and click **Save**.

Deleting a network bond

Follow these steps to delete a network bond.

To delete a network bond

1. From the **System topology** page on the Flex Appliance Console, click on each of your application instances and verify that the bond is not listed in the **IP address and interface pairs** field.
2. If the bond is listed for one or more instances, edit the network of each instance to remove the bond. You may need to add a different IP address and interface pair if the bond is the only interface that is assigned to the instance.

   See "Editing instance network settings" on page 87.

3. Navigate to the **Network interfaces** page and select the bond that you want to delete.
4. Click **Remove settings**.
5. Click **Delete bond**.

Configuring or editing a network interface

The information that you enter when you configure an interface is used to populate the network information fields when you perform operations on the Flex Appliance Console.

To configure or edit a network interface

1. Before you edit an existing network interface, first make sure that it is not in use by any application instances or for replication, as follows:

   - Navigate to the **Paired appliances** section of the **Remote replication** page. Verify that the interface is not listed under **Local appliance network interface**.

     If the interface displays in this field, edit the replication network to use a different interface. See "Editing the replication network" on page 117.

   - Navigate to the **Application instances** section of the **System topology** page. Click on each of your application instances and verify that the interface is not listed in the **IP address and interface pairs** field.

     If the interface is listed for one or more instances, edit the network of each instance to remove the interface. You may need to add a different IP address and interface pair if the interface that you want to edit is the only interface that is assigned to the instance. See "Editing instance network settings" on page 87.

   For both of these settings, if you do not have another available configured interface, use this procedure to configure an interface with placeholder values that you can use until you complete the edits.

2. On the Flex Appliance Console, click the **Network interfaces** icon in the left-side navigation bar to open the **Network interfaces** page.

   It may take a few minutes to load.

3. Do one of the following to enter network information:

   Note: If you configure a network interface with both IPv4 and IPv6 addresses, all instances that use the interface must also be configured with both IPv4 and IPv6 addresses.

   - If you want to use VLAN tagging, select the network interface and click **Add VLAN Tag**. Then enter a VLAN ID between 1 and 4,094 and at least one subnet and gateway pair. Use CIDR notation for the subnet and gateway. For example, 1.1.1.0/24.

     Do not enter the same VLAN ID or subnet and gateway pair for more than one interface.

Note: If you have more than one node, you must set the VLAN tag for each node.

- If you do not want to use VLAN tagging, click the name of the network interface, and then enter at least one subnet and gateway pair in CIDR notation. For example, 1.1.1.0/24.
  Do not enter the same subnet and gateway pair for more than one interface.

Note: The following subnets are reserved for internal use and cannot be used for the network interfaces:

192.168.227.0/24 and fdf8:192:168:227::/120

192.168.228.0/24 and fdf8:192:168:228::/120

192.168.229.0/24 and fdf8:192:168:229::/120

192.168.230.0/24 and fdf8:192:168:230::/120

4 Click **OK**.

See "Creating a network bond" on page 37.

Managing the appliance Fibre Channel ports

If your appliance has Fibre Channel ports, you can view and manage them from the **Fibre Channel interfaces** page on the Flex Appliance Console. To access the page, click the **Fibre Channel interfaces** icon in the left-side navigation bar.

On this page, you can view all of the Fibre Channel ports on the appliance. Click on any port to see additional information, such as the WWPN, the remote port, and the devices that are connected to it. See "Viewing the devices that are connected to the Fibre Channel ports" on page 43.

Note: The number of Fibre Channel ports on the appliance depends on your hardware configuration. For more information, see the *Product Description* for your specific hardware model.

This release supports the following types of backups over Fibre Channel:

- VMware SAN transport (initiator)
- Tape out (initiator)
- SAN client (Fibre Transport target)

If you want to perform backups over Fibre Channel, you must assign ports to your application instances. To assign or unassign ports, navigate to the **System topology** page and click on the instance name, then navigate to the **Fibre Channel** tab.

See "Assigning Fibre Channel ports to an instance" on page 92.

See "Unassigning Fibre Channel ports from an instance" on page 94.

Fibre Channel best practices

Cohesity recommends the following best practices for connecting Fibre Channel devices:

- Flex Appliance 7.0 has been tested for up to 6,000 storage devices or paths in the case of multipathing. If you zone more than the tested number of devices or paths, you may have to take additional steps to perform the following operations and avoid the associated issues:
  - Initial configuration and Flex Appliance updates
    These operations may take a long time or fail.
  - Factory reset
    During a factory reset, the Veritas Remote Management Interface may go blank and may not accept input.

  You should consult with Technical Support before you implement a Fibre Channel configuration of that size.
- VMware SAN transport mode only works with VMware Virtual Machine File System (VMFS) datastores version 6.0 or later. Other devices such as the raw device-mapping (RDM) format are not supported. Make sure that only VMFS devices are zoned to the appliance to avoid backup failures.
  Refer to the NetBackup Software Compatibility List to confirm the supported VDDK versions.
- Cohesity recommends that you do not allocate more than four ports to the same device unless the storage array requires it.
- If you run VMware SAN backups to LSI storage, the LSI storage should be configured in Asymmetric Logical Access Unit (ALUA) mode by following the procedure from the storage vendor. The procedure may involve updating the storage array firmware to a version that supports ALUA mode. If the storage was connected before it was configured in ALUA mode, you also need to unmap and remap the LSI storage LUNs to the appliance.
  After the LSI storage LUNs have been remapped, scan the associated Fibre Channel ports from the **Fibre Channel interfaces** page on the Flex Appliance Console.

- After an appliance restart or an instance relocation, monitor the **Fibre Channel interfaces** page and wait for the link state of the ports to be up before you run any backups. The ports may take up to 10 minutes to become active.

Viewing the devices that are connected to the Fibre Channel ports

You can view all the devices that are connected to the appliance Fibre Channel ports from the **Fibre Channel interfaces** page. You can also use this page to scan for new devices or clean stale device information from the system.

Use the following procedure to view the devices that are connected to a particular port.

To view the devices that are connected to a Fibre Channel port

1. On the Flex Appliance Console, click the **Fibre Channel interfaces** icon in the left-side navigation bar to access the **Fibre Channel interfaces** page.
2. Click on the port that you want to view the information for.
3. Under the **Devices** heading, click **Show**.

The appliance scans for devices when it starts up. Scanning a port that is already assigned to an instance does not require stopping the instance. Any devices added after the instance starts are automatically made available to the running instance once the scan completes.

A scan is also required if a SAN configuration change occurs, including device restarts or disconnections.

Note: You cannot scan the ports that are assigned to instances as targets for SAN client.

To clean a port that is assigned to an instance, you must stop the instance before performing the clean operation.

If you connect or remove devices while the appliance is running, use the following procedure to scan for newly connected devices or clean the removed devices from the system. When new devices are added, there may be a brief delay before they are detected during a scan.

To scan or clean Fibre Channel ports

1. On the Flex Appliance Console, click the **Fibre Channel interfaces** icon in the left-side navigation bar to access the **Fibre Channel interfaces** page.
2. Select the check box next to the port or ports that you want to scan or clean.
3. Click **Scan** or **Clean**.

Preserving MAC address for application instances

This feature enables application instances to retain the MAC address of the parent host interface across application stop and start events. Configuration is managed exclusively through an API endpoint.

Prerequisites:

- All application instances must be offline before toggling between **Auto** and **Preserve** modes.
- Only users with the **Change MAC Address Setting** permission are authorized to perform this operation.

Managing the configuration

The Preserve MAC address setting can be toggled between **Auto** and **Preserve** modes using API only. When the setting is enabled, a persistent informational message is displayed in the Flex Appliance console.

```
This appliance is configured to use the network interfaces'
 MAC addresses for the application instances.
```

The MAC address remains consistent across multiple stop/start cycles.

While the configuration is being applied across cluster nodes:

- Start and Relocate operations are blocked.
- Software updates are blocked until the appliance reaches a steady state.

Note: When a system reboot occurs during an active MAC address assignment operation, the activity monitor may display two tasks upon successful node recovery. The original task, which was initiated prior to the reboot event, will transition to a failed state due to process interruption. However, system continuity is maintained through an automated recovery mechanism that creates a new task post-reboot, ensuring that the MAC address configuration changes are successfully applied to the target interfaces.

Chapter 5

Managing users

This chapter includes the following topics:

Overview of the Flex Appliance default users

Flex Appliance comes with default users for the Flex Appliance Console, the Flex Appliance Shell, and the application instances.

The following list describes the default users and their functions:

- The **admin** user
  This user is the default user for the Flex Appliance Console. Use this user to sign in to the console for the first time. Once you do so, you are required to add a local user, and then the **admin** user is removed.
- The **hostadmin** user
  This user is the default user for the Flex Appliance Shell. Use this user to perform the initial configuration and for any other tasks that involve the shell.
- The **sysadmin** user

This user is the default user for the Veritas Remote Management Interface. Use this user and the remote management interface to access the Flex Appliance Shell for initial configuration, or as an alternative to an SSH session.

- The default application user
  Each application that is supported on Flex Appliance also has a default user. See the *NetBackup Application Guides* for specifics.

Managing Flex Appliance Console users and tenants

You can manage all of your Flex Appliance Console users from the **Access management** page. To access the **Access management** page, sign in to the console and click the **Access management** icon in the left-side navigation bar.

Users are assigned to tenants. A tenant is a separate space for a specific group of users and for a specific use. Different tenants can be allocated for different user groups.

See "Adding a tenant" on page 47.

Note: In this version of Flex Appliance, all users are assigned to all tenants.

User types

The following types of users are supported on the Flex Appliance Console:

- Local users
  See "Adding a local user to the Flex Appliance Console" on page 49.
- Active Directory and LDAP users
  See "Connecting a remote user domain to the Flex Appliance Console" on page 51.
- Single sign-on (SSO) users
  See "Managing single sign-on (SSO)" on page 53.
- Service accounts
  See "Managing service accounts" on page 78.

User access roles

User roles determine the access privileges that a user has on the Flex Appliance Console.

All users have the observer role by default except for the first local user that you add, which has the administrator and the security administrator roles. Users with

the security administrator role can assign additional roles from the **Access management** page. Select the user and click **Edit roles**.

The following base roles are available:

- Security administrator
  This role can manage users and oversee the security management of the appliance.
- Administrator
  This role can perform all but the security operations on the Flex Appliance Console.
- Observer
  This role can view all but the security information on the Flex Appliance Console. It cannot perform any operations.

The following extended roles are available:

- Application operator
  This role can start, stop, and relocate application instances.
- BIOS administrator
  This role can manage the BIOS password. It is available on appliances that support BIOS password protection.
  This role is not available in 5x7x appliance models.
- Security observer
  This role can view the security information on the Flex Appliance Console. It cannot perform any operations.
- SED Key Administrator
  This role manages the encryption keys that secure data on Self-Encrypting Drives.
  This role is available only on SED appliances.
- Support
  This role has access to view and manage the appliance logs.

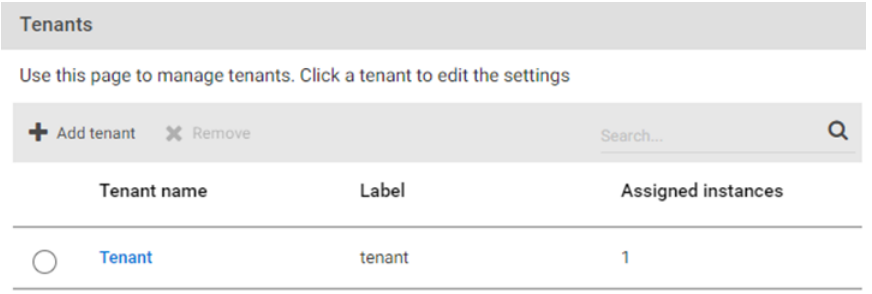
You can also create custom roles with user-defined access profiles that allow you to create specific permission sets beyond the default options.

Adding a tenant

Follow these steps to add a tenant.

To add a tenant

1 On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar to open the **Tenants** page.



2 Click **Add tenant**.

3 Enter a tenant name and location. Special characters are not allowed.

4 Complete the following network configuration settings:

Note: The network configuration information that you enter here is used to populate the network information fields when you create a new instance. You can also enter this information when you create an instance.

Domain name	Type the domain name for this tenant. You can enter only one domain name.
Search domains	To enter multiple search domains, type a comma and a space after each search domain.
Name servers	Type the IP addresses for the name servers for this tenant. To enter multiple name servers, type a comma and a space after each name server.
Hosts file entries	Type the `Hosts` file entries for this tenant if you do not want to use DNS or want to bypass DNS for specific hosts. Include entries for all hosts that you want your instances to communicate with.

5 Click **Save**.

After you add a tenant, you can assign instances to it.

Editing a tenant

Follow these steps to change the settings for a tenant.

To edit a tenant

1. On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar.
2. Click the name of the tenant that you want to edit.
3. Change the appropriate settings.
4. Click **Save**.

Removing a tenant

Follow these steps to remove a tenant.

To remove a tenant

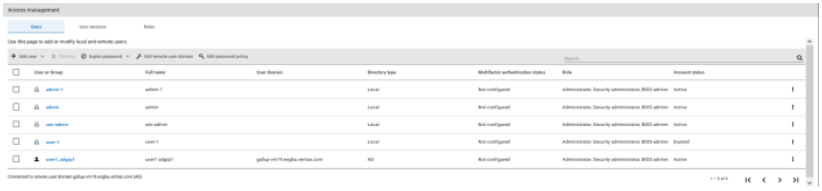
1. On the Flex Appliance Console, click the **Tenants** icon in the left-side navigation bar.
2. Select the tenant that you want to remove, then click **Remove**.

Adding a local user to the Flex Appliance Console

Follow these steps to add a local user.

To add a local user

1. On the Flex Appliance Console, click the **Access management** icon in the left-side navigation bar to open the **Access management** page.



2. Click **Add user** > **Add local user**.
3. Enter the requested information and click **Save**.

Creating custom roles

Custom roles in applications are user-defined access profiles that allow you to create specific permission sets beyond the default options. This flexibility ensures that users have exactly the rights needed for their jobs, reducing unnecessary access and improving security.

The **Roles** tab displays all available roles along with their type and description. By default, every role includes the Observer role.

To create a new custom role

1. Navigate to **Access Management > Roles**.
2. Select **Create role**.
3. Enter the role name and description.
4. Select the permissions that you want the role to have.
5. Click **Review**.
6. In the **Permissions for the Role** popup, review the selections and click **Create**.

The newly added role will appear on the **Access Management** page. Click the role name to view details of the permissions associated with it.

You can assign the newly created role to any user or group by navigating to **Access Management > Users** tab.

On the **Roles** tab, you can perform the following operations:

- View Usage: For any role, click **Action > View usage** to see the list of users assigned to the selected role and the multiperson authorization policies in which the role is designated as an approver.
- Copy and Customize: Select an existing role and click **Action > Copy and Customize** to create a new role based on it.
- Delete Role: For any role, click **Action > Delete**.

Note: Roles can be deleted only if they are not assigned to any user. Only custom roles can be deleted. Base and extended roles cannot be deleted.

Editing role assigned to a user

You can edit the roles that have been assigned to a user.

To edit a role assigned to a user

1. Navigate to **Access Management > Users**. The page lists all users.
2. Select the user whose role you want to edit and click **Action > Edit roles**.
3. In the **Edit roles** window, make the required changes and click **Save**.

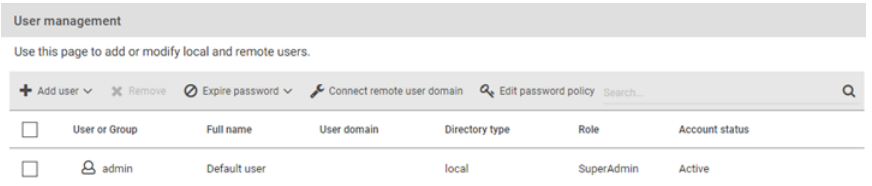
The user must sign out of any active console sessions and sign in again to see the updated permissions.

Connecting a remote user domain to the Flex Appliance Console

Follow these steps to connect an Active Directory (AD) or LDAP domain.

To connect a remote user domain

1. On the Flex Appliance Console, click the **Access management** icon in the left-side navigation bar to open the **Access management** page.



2. Click **Connect remote user domain**.
3. Fill in the required parameters and select the connection type. If you do not enter a **Port** value, the following default ports are used:
   - **Plain text** or **Plain text + TLS (encrypted)**: port 389
   - **SSL (encrypted)**: port 636
4. Select a directory type. If you select **OpenLDAP**, additional parameters appear. Make sure that these parameters match your LDAP server configuration.
5. When you are finished, click **Save**.

   If you selected the SSL connection type, a **Trust the certificate** window appears. Review the certificate details and click **Trust**.

Note: If you want to use an external certificate chain, you can upload it after you click **Trust**. When you return to the **Access management** page, click **Edit remote user domain** to upload the certificate chain. See “Editing a remote user domain in the Flex Appliance Console” on page 52.

Once the remote user domain has been connected, you can import remote users and user groups to grant them access to the Flex Appliance Console.

See "Importing a remote user or user group to the Flex Appliance Console" on page 52.

Editing a remote user domain in the Flex Appliance Console

Follow these steps to make changes to an Active Directory (AD) or an LDAP domain that is connected to Flex Appliance.

To edit a remote user domain

1. From the **Home** page of the Flex Appliance Console, click the **Access management** icon in the left-side navigation bar.
2. Click **Edit remote user domain**.
3. Modify the parameter fields as necessary and click **Save**.

   Note: If you upload an external certificate chain, the certificate's Subject Alternative Name (SAN) must match the server name or IP address that you entered.

4. If you changed the server name or the IP address, note the following information:
   - The existing remote user domain is overwritten with a new domain. Any imported users or user groups that are not part of the new domain are then unable to sign in. If you do not plan to add these users to the new domain, you can remove them from the **Access management** page.
     See "Removing user or service accounts from the Flex Appliance Console" on page 62.
   - If you previously uploaded an external certificate chain, it becomes invalid. After you save the server changes, return to the edit page to upload and trust a new certificate.

Importing a remote user or user group to the Flex Appliance Console

Follow these steps to import an Active Directory (AD) or LDAP user or user group.

Note: Nested user groups are not supported. To import the users of a nested group, you must perform this procedure for the group that they directly belong to.

To import a remote user or user group

1. On the Flex Appliance Console, click the **Access management** icon in the left-side navigation bar.
2. If you have not done so already, connect the remote user domain that the user or the user group belongs to.

   See "Connecting a remote user domain to the Flex Appliance Console" on page 51.
3. Click **Add user** > **Import remote users**.
4. Select **User** or **User group**.
5. Depending on your selection, enter the username or the group name. Do not include the domain name.
6. Click **Import**.

After you have imported the user or the user group, you can view the details on the **Access management** page.

Note: You cannot view the members of a user group from the Flex Appliance Console. Use the remote server to manage the users within a group.

Managing single sign-on (SSO)

The Flex Appliance Console supports single sign-on (SSO). Note the following prerequisites and considerations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported.
- SSO users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with a SAML-authenticated user.
- SSO users must use the fully qualified domain name (FQDN) in the URL to access the Flex Appliance Console. For example, **https://*consoleFQDN***. The IP address option does not work for SSO.
- Single logout (SLO) is supported if an SLO POST binding URL is present in the identity provider (IDP) metadata. If it is not present, you sign out only from the appliance and not from the IDP. In this situation, Cohesity recommends that you close your browser after signing out for security purposes.

Note: For some IDPs with SLO, you are not redirected to the sign-in page after you sign out of the console. Open a new session to sign back in.

Configuring SSO

Perform the following steps to configure SSO.

To configure SSO

1. Add the SSO identity provider (IDP).

   See "Adding an IDP" on page 55.

2. From the **Single sign-on** page, select the check box next to **Enable single sign-on** to enable SSO.

3. Import the SSO users that you want to have access to the Flex Appliance Console.

   See "Importing a remote user or user group to the Flex Appliance Console" on page 52.

Enabling or disabling SSO

Use the following procedure to enable or disable SSO. You must have added at least one IDP.

To disable or enable SSO

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.

2. Select or deselect the check box next to **Single sign-on**.

Managing identity providers (IDPs)

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol and AD or LDAP directory services. You can add up to three IDPs to the appliance but can use only one at a time.

Note: The date and time of the appliance, the IDP, and the browser must be synchronized. Cohesity recommends that the date and time are set using NTP.

Use the following procedures to manage your IDPs.

Adding an IDP

To add an IDP

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. Under **Appliance service provider URL**, copy or download the appliance metadata file. Upload that file to your IDP and add the appliance as a service provider. For more specific instructions, see the following articles on the Support website:
   - Active Directory Federation Services (ADFS)
   - IBM
   - Microsoft Azure Active Directory
   - Okta
   - Ping Federate
   - Shibboleth
3. From the IDP, download and save the IDP metadata XML file.
4. Gather the following information for the IDP:
   - Name: A name of your choosing to identify the IDP.
   - User field: The SAML attribute name that is mapped to the user attribute of the remote user domain. For example, **userPrincipalName**, **displayName**, **identifier**, **uid**, etc.
   - Group field: The SAML attribute name that is mapped to the group attribute of the remote user domain. For example, **memberOf**, **role**, etc.
5. From the **Single sign-on** page on the Flex Appliance Console, click **Add**.
6. Upload the IDP metadata file. Once the file has uploaded successfully, click **View details** and verify the certificate subject values and SHA-256 fingerprints.
7. Fill in the other required fields, then click **Save**.
8. If you have added only one IDP, enable SSO to start using it. See “Enabling or disabling SSO” on page 54.

   If you have added more than one IDP, the first IDP is used by default. Switch to the new IDP if necessary. See “Switching to a different IDP” on page 56.

Editing an IDP

To edit an IDP

1. If you need to change the IDP metadata XML file, download the file from the IDP.
2. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
3. Click the name of the IDP, then click **Edit**.
4. Make the required changes. If you uploaded a new IDP metadata file, click **View details** and verify the certificate subject values and SHA-256 fingerprints.
5. When you are done, click **Save**.

Switching to a different IDP

To switch to a different IDP

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. If you have not done so already, add the IDP that you want to use. See "Adding an IDP" on page 55.
3. Make sure that SSO is enabled. Then select the IDP that you want to use and click **Use**.

Removing an IDP

To remove an IDP

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Single sign-on**.
2. Select the IDP that you want to remove and click **Remove**.

Note: If you have more than one IDP, you cannot remove the one that is in use unless you remove the others first. If you have only one IDP or have already removed the others, you must disable SSO before you can remove it. See "Enabling or disabling SSO" on page 54.

Importing a single sign-on user or user group to the Flex Appliance Console

Follow these steps to import a single sign-on (SSO) user or user group.

Note: Nested user groups are not supported. To import the users of a nested group, you must perform this procedure for the group that they directly belong to.

To import an SSO user or user group

1. On the Flex Appliance Console, click the **Access management** icon in the left-side navigation bar.
2. If you have not done so already, add the SSO identity provider (IDP) and enable SSO.

   See "Managing identity providers (IDPs)" on page 54.

   See "Managing single sign-on (SSO)" on page 53.
3. Click **Add user** > **Import single sign-on (SSO) users**.
4. Select **User** or **User group**.
5. Depending on your selection, enter the username or the group name in the format ***<user or group>@<domain>***. Note that the parameters are case sensitive. For example, **User@example.com** or **group@example.com**.

   If a group or user has multiple common names (CNs) in their distinguished name (DN), enter them as a directory path. For example, if the DN is `CN=testgroup,CN=Users,DC=example,DC=com`, enter **Users/testgroup@example.com**.
6. Click **Import**.

After you have imported the user or the user group, you can view the details on the **Access management** page.

Note: You cannot view the members of a user group from the Flex Appliance Console. Use the IDP to manage the users within a group.

Managing user authentication with smart cards or digital certificates

You can use smart cards or certificates for user validation with a remote user domain. This authentication method is not available for local users.

Note: Smart card authentication does not apply for users who have configured multifactor authentication.

Prerequisites

Note the following prerequisites for smart card authentication:

- DNS must be configured on the appliance.
  See “Changing DNS or Hosts file settings” on page 157.
- The remote users who are associated with the smart cards or digital certificates must be imported to the appliance.
  See “Importing a remote user or user group to the Flex Appliance Console” on page 52.
- Cohesity recommends that the appliance date and time are set using NTP.
  See “Setting the date and time for appliance nodes” on page 35.

Configuring or editing smart card authentication

Follow these steps to configure user authentication with smart cards or digital certificates or to edit an existing configuration.

To configure or edit smart card authentication

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.
2. Click **Configure** or **Edit**.
3. Select a certificate mapping attribute and optionally enter the OCSP URI. If you do not provide the OCSP URI, the URI in the certificate is used.
4. Browse for or drag and drop the CA certificates that are associated with the user smart cards or the user digital certificates. Certificate file types must be in `.pem` format and less than 1,000 KB in size.

   To remove a certificate, click the **x** next to the file name. If the certificate is part of a certificate chain, make sure that you also remove the other certificates in the chain.

   Note: If you use Mozilla Firefox, you must also remove the certificate from the browser's certificate manager. See the browser documentation for instructions.

5. Click **Save**.
6. Open a new session to the Flex Appliance Console. The sign-in page should now display an option to sign in with a certificate or smart card.

7 Before a user can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager. See the browser documentation for instructions.

8 Once a user inserts a smart card or uploads a certificate, they are prompted to select and authenticate the certificate when they open a new session to the Flex Appliance Console. Once they do so, they can use the certificate to sign in.

   If the user does not select and authenticate the certificate when prompted, they can still sign in with their username and password.

Disabling or enabling smart card authentication

Follow these steps to disable user authentication with smart cards or digital certificates or to enable it after it has been disabled.

To disable or enable smart card authentication

1 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Smart card authentication**.

2 Click **Disable** or **Enable**.

If you disable smart card authentication, users no longer see an option to sign in with a certificate or smart card.

Changing a local user password in the Flex Appliance Console

Follow these steps to change the password of a local user.

Note: Remote user passwords cannot be changed from the Flex Appliance Console. They must be changed from the server on which they reside.

To change a user password

1 Sign in to the Flex Appliance Console from the user account that you want to change the password for.

2 In the top-right corner of the screen, click the black circle icon that includes the user's initials. For example, if the user's full name is Default User, the icon includes the initials DU.

3 Click **Change password**.

4 Fill in the required fields. The password must adhere to the current password policy.

See “Changing the password policy” on page 62.

5 Click **Save**.

Expiring local user passwords in the Flex Appliance Console

Expiring a user password forces that user to change their password the next time that they sign in to the Flex Appliance Console. If the user is currently signed in, the current session is not affected.

Use the following procedure to expire the password for local users.

To expire user passwords

1 Sign in to the Flex Appliance Console as a security administrator.

2 Click the **Access management** icon in the left-side navigation bar to open the **Access management** page.

3 Do one of the following:

- To expire the password for a specific user or users, select the user or users and click **Expire password** > **Expire selected users**.
- To expire the password for all users, click **Expire password** > **Expire all users**.

Note: If you expire your own password, you are immediately signed out of the Flex Appliance Console.

Unlocking a user account in the Flex Appliance Console

The Flex Appliance Console is protected with the following account locks:

- Local user accounts become locked after three sign-in attempts with incorrect passwords. If a security administrator account becomes locked, it is unlocked automatically after 30 minutes. If a different local user account becomes locked, that user and a security administrator must work together to unlock it.
- Accounts with multifactor authentication become locked after three sign-in attempts with incorrect codes. The account unlocks automatically after 15 minutes.

Use the following procedures to unlock a locked user account. You can use these procedures for situations where the account unlocks automatically, but note that once you start the manual unlock, the automatic unlock is canceled.

Steps for the security administrator

The security administrator must generate a secure unlock code for the locked user.

To generate a secure unlock code

1. Sign in to the Flex Appliance Console and click the **Access management** icon on the left.
2. Locate the locked user in the table and click **Unlock**.
3. Copy the code and send it to the local user. The code is valid for 24 hours. If you generate a new code during that time, the first one becomes invalid.

Steps for the locked user

Once the security administrator has sent the secure unlock code, the locked user can unlock their account.

To unlock a user account

1. Open a session to the Flex Appliance Console, enter your username and password, and click **Sign in**.
2. You are redirected to a page to enter your secure unlock code. Enter the code that you received from the security administrator and click **Confirm**.
3. On the page that appears, enter your current password and a new password.
4. Use the new password to sign back in to the Flex Appliance Console.

Managing open sessions

You can manage your open sessions from the **Open sessions** page, or a security administrator can manage all open sessions from the **Access management** page. Open sessions include sign-in sessions on the Flex Appliance Console and API sessions with a personal API token.

Use the following procedures to manage open sessions.

To manage your own sessions

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Manage open sessions**.

   The **Open sessions** page appears and shows all of your open sessions.

2. To sign out of a specific session, locate the session and click **Actions** > **Sign out**.

   To sign out of all open sessions, click **Sign out of all sessions**.

To manage all sessions

1. Sign in to the Flex Appliance Console as a security administrator and click the **Access management** icon on the left.
2. On the **Access management** page, navigate to the **User sessions** tab. This tab shows all open sessions for all accounts.
3. To sign out of a specific session, locate the session and click **Actions** > **Sign out**.

   To sign out of all open sessions, click **Sign out of all sessions**.

Removing user or service accounts from the Flex Appliance Console

Follow these steps to remove user or service accounts.

Note: Users cannot remove their own user accounts.

To remove user or service accounts

1. On the Flex Appliance Console, click the **Access management** icon in the left-side navigation bar.
2. To remove a single account, locate the account that you want to remove and click **Actions** > **Remove user account** or **Actions** > **Delete service account**.

   To remove multiple accounts, select the accounts that you want to remove and click **Remove**.

Changing the password policy

You can use the Flex Appliance Console to edit the password policy for user passwords. The password policy is enforced for local Flex Appliance Console users and the **hostadmin** user in the Flex Appliance Shell.

The default password policy is as follows:

Password complexity:

- Minimum characters: 8
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 0
- Minimum different characters: 0
- Maximum consecutive repeating characters: 99999
- Maximum consecutive characters of the same type: 99999

Password age:

- Days before password must be changed: 99999
- Days before password can be changed: 0
- Days before password expires to display warning message: 10
- Minimum different passwords before allowing reuse: 7

Use the following procedure if you need to make changes to this policy.

To edit the password policy

1. Sign in to the Flex Appliance Console as a security administrator.
2. Click the **Access management** icon in the left-side navigation bar to open the **Access management** page.
3. Click **Edit password policy**.
4. If you want your password policy to adhere to the Security Technical Implementation Guides (STIGs), select the **Use STIG for validation** toggle. You can click **Reset to STIG default** to fill in the default values for all fields.
5. Fill in or adjust the required parameters as needed, then click **Save**.

Changing the hostadmin user password in the Flex Appliance Shell

Follow these steps to change the **hostadmin** user password.

To change a hostadmin user password

1. Log in to the Flex Appliance Shell, and then type the following:

   ```
   set user password
   ```

2. Press **Enter**.
3. Type a new password.

   The password must adhere to the password policy that is set on the Flex Appliance Console. In addition, dictionary words are not accepted.

   See "Changing the password policy" on page 62.

Changing the sysadmin user password in the Veritas Remote Management Interface

Follow these steps to change the **sysadmin** user password.

To change the sysadmin user password

1. Log in to the Veritas Remote Management Interface.
2. Navigate to **Configuration** > **Users** and select the **sysadmin** user.
3. Click **Modify User**.
4. Select the **Change Password** check box and enter a new password.

Managing multifactor authentication

Flex Appliance supports multifactor authentication for local, Active Directory (AD), and LDAP users in the Flex Appliance Console and the **hostadmin** user in the Flex Appliance Shell. Multifactor authentication uses time-based one-time passwords to provide secure authentication. Each user can configure multifactor authentication individually, or a security administrator can enforce multifactor authentication for all console users.

Multifactor authentication does not apply for users who have configured smart card authentication or for SSO users. For SSO users, Cohesity recommends that you configure multifactor authentication through the SSO identity provider (IDP).

Note: AD and LDAP user groups are not supported for multifactor authentication. You can add these users individually so they can configure multifactor authentication, or you can configure authentication with smart cards or digital certificates instead.

See “Configuring or reconfiguring multifactor authentication” on page 65.

See “Enforcing multifactor authentication” on page 67.

Configuring or reconfiguring multifactor authentication

Flex Appliance supports multifactor authentication for local, Active Directory (AD), and LDAP users in the Flex Appliance Console and the **hostadmin** user in the Flex Appliance Shell.

The following authenticator apps are supported:

- Microsoft Authenticator version 6.5.12 and later
- Google Authenticator
- Okta Verify
  Note that when you scan the QR code with this app, the authentication process could take up to a minute.
- Symantec VIP Access 4.3.3 and later

Note: Multifactor authentication may affect integrations like APIs, automation, and third-party Privileged Access Management (PAM) solutions.

Configuring or reconfiguring multifactor authentication for the Flex Appliance Console

Before you can configure multifactor authentication for a user in the Flex Appliance Console, the following prerequisites must be met:

- The appliance date and time must be set with NTP.
- At least one user must have the security administrator role. If you are the user with the security administrator role, at least one additional user must also have the security administrator role.
- You must have a supported authenticator app installed on your mobile device.

To configure or reconfigure multifactor authentication for the Flex Appliance Console

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Configure multifactor authentication**.
2. On the **Configure multifactor authentication** page, click **Configure** or **Reconfigure**.
3. Follow the prompts to add your Flex Appliance account to the authenticator app.

   If you have already configured multifactor authentication for another appliance and want to use the same authenticator account to sign in to this appliance, select the option **Use a custom key**. Enter the key from the appliance that is already configured.

   You can also create and enter your own key with the custom key option. If you create your own key, note that some authenticator apps may not support pad characters. Confirm compatibility with your app if you want to use them.

Configuring or reconfiguring multifactor authentication for the Flex Appliance Shell

Before you can configure multifactor authentication for the **hostadmin** user in the Flex Appliance Shell, the following prerequisites must be met:

- The appliance date and time must be set with NTP.
- You must have a supported authenticator app installed on your mobile device.

To configure or reconfigure multifactor authentication for the Flex Appliance Shell

1. From the Flex Appliance Shell, run the following command:

   ```
   set user mfa
   ```

2. Follow the prompts to add the **hostadmin** account to your authenticator app.

   If you have already configured multifactor authentication for another appliance and want to use the same authenticator account to sign in to this appliance, respond **yes** to the question **Do you want to specify an existing key?** Enter the key from the appliance that is already configured. You can view the key on the other appliance with the `show user mfa key` command.

   You can also create and enter your own key with the existing key option. If you create your own key, note that some authenticator apps may not support pad characters. Confirm compatibility with your app if you want to use them.

3. Share the QR code or the key with anyone else who requires access to the Flex Appliance Shell so that they can also add the **hostadmin** account to their authenticator app. You can view the QR code and the key at any time with the following command:

   ```
   show user mfa key
   ```

4. If you have a multi-node appliance, repeat these steps on the other node.

Enforcing multifactor authentication

You can enforce multifactor authentication for users in the Flex Appliance Console, so that they must configure it by the date that you select.

Note: Remote AD and LDAP user groups are not supported when multifactor authentication is enforced. Once you enforce it, users in these groups can no longer sign in.

You cannot enforce multifactor authentication for the **hostadmin** user in the Flex Appliance Shell.

You also have an option to opt out of multifactor authorization.

Before you can enforce multifactor authentication, the following prerequisites must be met:

- The appliance date and time must be set with NTP.
- You and at least one other user must have the security administrator role. At least one of the users with the security administrator role must be a local user.
- You must have multifactor authentication configured on your account.

Note that:

- After a new installation of Flex Appliance, the **Enforce multifactor authentication** enforcement dialog will appear at every login until the administrator explicitly enforces or opts out. If the dialog is closed without making a choice, the user remains on the home page, and the **Enforce multifactor authentication** screen will reappear on subsequent logins. An opt-out without providing a reason is treated as no choice, so the dialog continues to appear at each login.
  This is the default state of the appliance.
- If the prerequisites are met and no selection is made, the **Enforce Multifactor authentication** option is selected by default and the enforce date popup is automatically shown. You can close the date selection screen and choose opt-out at this point.

- If the prerequisites are not met, you cannot enforce multifactor authentication. But you can opt out of multifactor authentication. Once the prerequisites are met, you can choose to enforce multifactor authentication even if you opted out of it before.
- If you have enforced multifactor authentication but the enforcement is not effective, you can change the effective date but you cannot change the configuration.

To enforce multifactor authentication

1. Sign in to the Flex Appliance Console as a security administrator. Click the **Settings** icon in the top-right corner of the page and then click **Multifactor authentication enforcement**.
2. On the **Multifactor authentication enforcement** page, click **Enforce**.
3. Select a start date within the next 90 days.

   Caution: Once you enforce multifactor authentication, you cannot cancel the enforcement or extend the start date past 90 days.

4. Click **Enforce**.

If you need to change the start date, return to the **Multifactor authentication enforcement** page and click **Edit enforcement**.

To opt out of multifactor authentication

1. Go to **Settings > Multifactor authentication enforcement** and select **Opt-out of Multifactor Authentication (MFA)**.
2. The **Multifactor Authentication Liability Agreement** popup appears. The popup will walk you through the liability agreement. Read and accept the liability agreement. Click **Next**.
3. Select the reason for opting out of multifactor authentication. You can choose any of the listed options or choose **Custom** and specify the reason for opting out.
4. Click **Confirm**.

Resetting multifactor authentication

If a user with multifactor authentication changes or loses access to their mobile device and cannot sign in, use one of the following procedures to reset multifactor authentication for that user. After a reset, the user is forced to reconfigure multifactor authentication the next time that they sign in.

Resetting multifactor authentication for a Flex Appliance Console user

To reset multifactor authentication for a Flex Appliance Console user

1. Sign in to the Flex Appliance Console as a security administrator and navigate to the **Access management** page.
2. Click the Actions menu to the right of the user that you need to reset and click **Reset multifactor authentication**.

Resetting multifactor authentication for the hostadmin user in the Flex Appliance Shell

If multifactor authentication for the **hostadmin** user is configured on more than one mobile device, you may not need to reset multifactor authentication if you lose access. Instead, ask someone who still has access to share the QR code or the key and use them to add the account back to your authenticator app.

The other user can view the QR code and the key with the following command in the Flex Appliance Shell:

```
show user mfa key
```

If no other devices have access, use the following procedure to reset multifactor authentication for the **hostadmin** user.

To reset multifactor authentication for the hostadmin user in the Flex Appliance Shell

1. Sign in to the Flex Appliance Console as a security administrator.
2. Click the **Help and support** icon in the top-right corner of the page. Under **Reset multifactor authentication**, click the **hostadmin** user for the node that you need to reset.

Disabling multifactor authentication

Use the following procedures to disable multifactor authentication after it has been configured.

Note: If multifactor authentication is enforced, Flex Appliance Console users cannot disable it after the start date.

To disable multifactor authentication for the Flex Appliance Console

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Configure multifactor authentication**.
2. On the **Configure multifactor authentication** page, click **Disable**.

To disable multifactor authentication for the Flex Appliance Shell

1. Log in to the Flex Appliance Shell.
2. Run the following command:

```
delete user mfa
```

Managing multiperson authorization

Multiperson authorization is a security mechanism designed to proactively protect data and systems from undesirable or malicious actions by a compromised insider acting alone. With multiperson authorization enabled, certain critical operations require approval from additional authorized users before execution. Even if a user has permission under role-based access control to perform an operation, the action will only proceed after additional authorized users review and approve it. This ensures accountability and reduces the risk of unauthorized changes.

The multiperson authorization policy defines who can review and approve an operation. Importantly, the multiperson authorization policy itself is protected by multiperson authorization, ensuring that policy changes also require quorum approval.

The multiperson authorization access control policy applies to the following operations:

- Editing user roles
- Removing users
- Editing, disabling, or deleting policies

Note: Custom policies in multiperson authorization are currently supported only for SED operations.

Flex Appliance operations for which you can configure multiperson authorization

Multiperson authorization can be configured for the following operations:

- Edit KMS operation
- SED switch and rekey operation

Terminology

- Request - A multiperson authorization request to perform a critical operation.

- Requester - A user who wants to perform a critical operation that requires multiperson authorization.
- Approver - An individual who reviews and allows an operation that requires multiperson authorization by approving a request.
- Exempted user - A user who does not need multiperson authorization for operations except the following:
  - To modify multiperson authorization configuration
  - To modify security properties

  This eliminates the necessity for any approvals. However, it must be used with caution. If the exempted user account is hacked, the multiperson authorization process can be of no use as it is bypassed for this user. For additional security, it is recommended that there are no exempted users.

  Note: Exempted users are currently supported only for SED operations.

- Expiration period - It is a configurable option that defines the duration for which a multiperson authorization request can be in the Pending state. A request expires if it is in the Pending state for more than the configured expiry period. Expiration period can vary from minimum 48 hours to 168 hours.
- Deletion period - It is a configurable option that defines the period (in days) after which requests will be deleted when no action is performed on them. Deletion period can range from 7 to 180 days..

Multiperson authorization process workflow

The process workflow for multiperson authorization is as follows:

1. A requester performs a critical operation using the Flex Appliance Console.
2. A request is created.
3. The request is pending for approval
4. Approvers review the request.
5. Approvers either approve or reject the request.
6. After the quorum is reached, the request is scheduled by Flex Appliance and finally marked as Done after the execution.
7. The request activity log, request, and response details can be viewed by the approver or the requester using the Flex Appliance Console on the **Request management** page.

8. A request is expired after it ages beyond the expiration period. It has to be created again, if required.
9. All requests in the Done, Rejected, Expired, and Canceled states are deleted when the retention period has elapsed.
10. All requests in the Pending state are expired when they reach the expiration period.

Considerations for configuring multiperson authorization

Prerequisites:

- At least three security administrators are required to enable multiperson authorization.

Note that:

- Security administrators can enable, disable, and edit access control policies.
- Service accounts cannot approve pending requests.
- Policy creator cannot exempt themselves during creation.
- Notifications are sent to specified email recipients for approval requests.
- The number of approvals required can range from 2 to 10.
- Pending requests can be cancelled by the requester.
- Security administrators can deny any pending requests.
- Security observers can view all policies and pending requests.
- Other users can view requests they created or can approve.
- Quorum is evaluated independently for each approver role. If a single user holds multiple approver roles defined in the policy, that user's approval counts toward the quorum for each role they hold.

The following considerations apply only to SED appliances:

- A custom policy can be created only after the access control policy is enabled.
- If a custom policy exists, the access control policy cannot be disabled.
- When a custom policy is created, it must have at least one operation. It is possible to edit an existing custom policy and remove all the operations.
- To enable multiperson authorization for an operation, it must be added to a new or existing custom policy.
- Security administrators can create, edit, or delete custom policies. Users with custom roles can also perform these operations if they have the permission.

- Creating a new custom policy does not require multiperson authorization approval; editing or deleting a custom policy requires quorum from other security administrators.
- When an operation is removed from a custom policy, any pending requests for that operation are automatically rejected.

Configuring multiperson authorization

You can navigate to the **Multiperson authorization** in any of the following ways:

- Navigate to **Settings > Security and compliance > Multiperson authorization**.
- On the Home page, select **Security meter**. In the **Security recommendations** pop-up, select **Multiperson authorization**.

The following table lists the operations that can be performed on an access control policy.

Table 5-1

Operations	Procedure
Enable access control policy	Enabling access control policy
Edit access control policy	Editing an access control policy
Disable access control policy	Disabling access control policy
Create multiperson authorization policy **Note:** This can be done only on an SED appliance.	Creating multiperson authorization policy
Delete custom policy **Note:** This can be done only on an SED appliance.	Deleting custom policy
View multiperson authorization requests	Viewing multiperson authorization requests
Manage multiperson authorization requests	Managing multiperson authorization requests

Enabling access control policy

To enable access control policy

1. Navigate to **Multiperson authorization**.
2. Click **Enable**.
3. Confirm the change.

A request is created. Once it is approved, the access control policy is enabled.

You can edit and disable access control policies.

Editing an access control policy

To edit an access control policy

1. Navigate to **Multiperson authorization**.
2. Click **Edit**.
3. You can update any of the following fields:
   - Email addresses: Specify a comma-separated list of email addresses for notifications.
   - Expire pending requests after: Set the period (in hours) after which any pending requests will expire.
   - Delete resolved requests after: Specify the period (in days) after which resolved requests will be deleted.
4. Click **Save**.

A request is created. Once it is approved, the access control policy is updated with the changes.

Disabling access control policy

To disable access control policy

1. Navigate to **Multiperson authorization**.
2. Click **Disable**.
3. Provide a reason in the pop-up and click **Disable**.

A request is created. Once it is approved, the access control policy is disabled.

Viewing multiperson authorization requests

The **Multiperson Authorization** widget appears on the Homepage when there are one or more pending authorization requests that require user attention. The widget provides a quick snapshot of requests you have submitted as well as requests awaiting your review.

Note: The counts displayed in the V**iew Requests** section on the dashboard and in **My Actions** reflect only active requests. They exclude requests in Done, Rejected, Expired, or Canceled states.

Viewing multiperson authorization requests

1. On the Home page, select **View requests** in the **Multiperson authorization** widget.
2. The **Request management** page lists all your requests for operations that require multiperson authorization. You can apply filters to view requests that you have submitted, requests sent to you for approval, and to narrow results by time frame or request status.
3. Select the request ID to see the request details. The **Audit trail** tab gives more details on the status of your request.
4. Select the **Preview request details** tab to see the changes that have been made as part of the request.

   The requester can cancel his request by selecting **Cancel request**.

Users with the approver role can approve or reject the multiperson authorization requests.

Managing multiperson authorization requests

To manage multiperson authorization requests

1. On the Home page, select **My actions** in the **Multiperson authorization** widget.

   You can also click on the User icon on the top right corner. In the pop-up, select the **View authorization request** option.
2. The **Request management** page lists all the requests for operations that require multiperson authorization. You can apply filters to view requests that you have submitted, requests sent to you for approval, and to narrow results by time frame or request status.
3. Select the request ID to see the request details. The **Audit trail** tab gives more details on the request. The **Preview request details** tab to see the changes that have been made as part of the request.
4. Select **Approve** if you want to approve the request. In the **Approve request** pop-up, provide the reason for approving the request. Click **Approve** to complete the approval.

   Select **Reject** if you want to reject the request. In the **Reject request** pop-up, provide the reason for rejecting the request. Click **Reject** to complete the rejection.

   The reason field can contain 8–256 characters and may include only alphanumeric characters, spaces, periods, commas, underscores, and dashes.
5. The **Request details** page gets updated with the details.

Creating multiperson authorization policy

You can create a multiperson authorization policy only on an SED appliance.

To create a multiperson authorization policy

1. Navigate to **Multiperson authorization**.
2. In the **Custom policies** panel, click **Create**.
3. In the **Create multiperson authorization policy** window, enter the following details:
   - Policy name: Specify the policy name.
   - Expire pending requests after: Set the period (in hours) after which any pending requests will expire.
   - Email addresses: Specify a comma-separated list of email addresses for notifications.
   - Exempted accounts: Specify accounts that are exempted from multiperson authorization (if any).
   - Delete resolved requests after: Specify the period (in days) after which resolved requests will be deleted.
   - Approvers: Specify the approvers.
   - Number of approvals: Specify the number of approvals required.
   - Under **Operations**, select the operations that require multiperson authorization.
   - Under **Behavior after approval**, choose any option:
     - **Automatically**: The requested operation will be completed automatically after approval.
     - **Manually**: The requested operation will have to be completed manually after approval. Navigate to the **Request management** page. Select the request and click **Complete operation**.
4. Click **Create**.
5. In the confirmation pop-up, review the information and click **Create**.
6. Click **Save**.

After the quorum is reached, the request is scheduled by the Flex Appliance and marked as Done after execution.

The new policy details appears on the **Multiperson authorization** page.

You can also edit an existing multiperson authorization policy. Click the policy name to open the Edit window. Make the required changes and save the changes.

Deleting custom policy

You can delete a custom policy only on an SED appliance.

To delete a custom policy

1. Navigate to **Settings > Security and compliance > Multiperson authorization**.
2. The **Multiperson authorization** page lists all the custom policies.
3. You can delete the custom policy by clicking **Delete** on the right side of the row.
4. Provide confirmation in the pop-up.

A request is created. Once it is approved, the access control policy is deleted.

Using Flex Appliance Console accounts for API automation

Flex Appliance includes the following features that you can use to manage or monitor your appliances through API automation:

- Personal API tokens
  You can generate a personal API token for an account and use that token for API access. Each account can have a maximum of one personal API token, and you can revoke it or change the expiration at any time.
  See “Managing personal API tokens” on page 77.
- Service accounts
  You can convert a regular user account to a service account that can only be used for API access. It does not have access to the Flex Appliance Console. A service account can have any number of tokens, but they cannot be revoked. The token expiration is determined by the maximum token validity that you set.
  See “Managing service accounts” on page 78.

Managing personal API tokens

You can generate a personal API token for a user account and use that token for API access. The personal API token has the same access permissions as the account. Check SORT for more information on the APIs.

Note: You can also generate a personal API token for a service account but must do so through the APIs.

Use the following procedures to manage personal API tokens.

To generate a personal API token

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Generate personal API token**.
2. Fill in the required fields and click **Generate**.
3. Follow the instructions to copy the key to a safe location.

To change the token expiration or reissue it if it has expired

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Manage personal API token**.
2. Click **Change expiration** or **Reissue**.
3. Fill in the required fields and click **Save** or **Reissue**.

To revoke a token or delete it if it has expired

1. From the Flex Appliance Console, click your user icon in the top-right corner and click **Manage personal API token**.
2. Click **Revoke** or **Delete**.
3. In the confirmation window that appears, click **Revoke** or **Delete**.

Managing service accounts

You can convert a Flex Appliance Console user account to a service account that you can use for API automation. A service account does not have access to the Flex Appliance Console. Check SORT for more information on the APIs.

Use the following procedures to manage service accounts.

To convert a user account to a service account

1. Sign in to the Flex Appliance Console as a security administrator and click the **Access management** icon on the left.
2. Locate the user account that you want to convert. Click **Actions** > **Convert to service account**.
3. Enter a maximum token validity for the account and click **Convert**.

To change the maximum token validity

1. Sign in to the Flex Appliance Console as a security administrator and click the **Access management** icon on the left.
2. Locate the user account that you want to modify. Click **Actions** > **Change token validity**.
3. Enter the new maximum token validity and click **Change**.

Chapter 6

Using Flex Appliance

This chapter includes the following topics:

Managing the repository

Before you can create an application instance, install an application add-on, or update the appliance software, you must first add the applicable files to the repository.

To access the repository, sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar.

The **Repository** page consists of the following tabs:

- **Applications**
  Use this tab to manage your applications for creating and upgrading instances. The tab displays the applications that are in the repository and their versions.
- **Application add-ons**

Use this tab to manage application add-ons for your instances. The tab displays the add-ons that are in the repository and details about each, such as type, version, and the application they can be installed on.

- **Appliance updates**
  Use this tab to manage update packages for Flex Appliance. The repository can only hold one update package at a time. The tab displays the package that is currently in the repository and details relevant to installing the update.

Use the Repository tabs to do the following:

- Add files to the repository
  See "Adding files to the repository" on page 81.
- Remove files from the repository
  See "Removing files from the repository" on page 82.
- Update Flex Appliance

Adding files to the repository

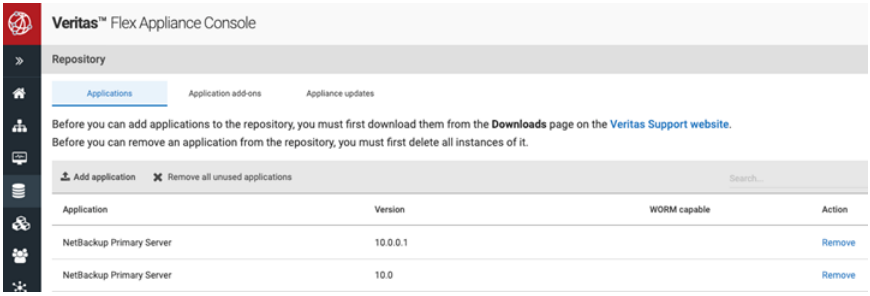
Use the following procedure to download and add files to the Flex Appliance repository.

Guidelines for adding files to the repository:

- Only add files that have been downloaded from or provided by Cohesity.
- Do not change the file names.
- To avoid upload issues, ensure that your computer has a strong network connection with the appliance and is connected locally to the same network. Cohesity recommends that you use a Windows lab computer if available.

To download and add files to the repository

1. From a computer within your appliance domain, download the appropriate file from the Download Center on the Support website.
2. From the same computer, sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar to open the **Repository** page.



3. On the **Repository** page, navigate to the **Applications**, **Application add-ons**, or **Appliance updates** tab, depending on the type of file that you want to add.
4. Click **Add application**, **Add add-on**, or **Add package**.
5. In the dialog box that appears, do the following:
   - At the top of the dialog box, click on the drop-down and navigate to the location where you downloaded the file.
   - Select the downloaded file from the list of items that appears, then click **Open**.

   If you added an update package, a progress banner appears at the top of the screen. When the task is complete, the new file appears on the page.

   If you added an application or application add-on, you are redirected to the Activity Monitor to view the progress. When the task is complete, return to the **Repository** page to see the new file at the top of the list.

Removing files from the repository

Use the following procedure to remove files from the Flex Appliance repository.

To remove files from the repository

1. Sign in to the Flex Appliance Console and click the **Repository** icon in the left-side navigation bar.
2. On the **Repository** page, navigate to the tab for the type of file that you want to remove.
3. Do one of the following:
   - To remove an application, locate the row of the application that you want to remove and click **Remove**. You can also click **Remove all unused applications** to remove all of the applications that are not currently in use. You can also remove the unused add-ons that correspond to the application. To do so, select **Remove corresponding unused add-ons** in the confirmation window that appears. Then click **Remove**.
   - To remove an add-on, locate the row of the add-on that you want to remove and click **Remove**. You can also click **Remove all unused add-ons** to remove all of the add-ons that are not currently installed on application instances.
   - To remove an update package, click **Remove package**.

Creating application instances

You can create application instances from the **System topology** page of the Flex Appliance Console. Navigate to the **Application instances** section and click **Create instance** to open a new page that leads you through the instance creation process.

Note: You also need to complete additional configuration steps from within NetBackup. See the *NetBackup Application Guides* for detailed instructions for your specific version of NetBackup.

Depending on the application version, you can create instances of the following applications:

- NetBackup primary server
  You can also configure a BMR primary server with this application. However, the BMR boot server cannot be configured on the appliance.
- NetBackup media server with the following storage options:
  - Media Server Deduplication Pool (MSDP)
    You can also configure MSDP cloud storage with this application. Refer to the *NetBackup Deduplication Guide* after the instance is created.

  - AdvancedDisk
- NetBackup WORM storage server

The NetBackup applications must follow the same compatibility requirements between NetBackup versions as any other NetBackup environment. See the *NetBackup Release Notes* for specifics.

For a full list of supported applications and versions for each Flex Appliance release, see the following article on the Support website:

Flex Appliance supported applications and usage information

Managing application instances from Flex Appliance and NetBackup

After you have created your instances, the instance management is divided between Flex Appliance and NetBackup, depending on the type of operation. In general, use Flex Appliance for any tasks that are related to the appliance or the application files. Use NetBackup for any tasks that are related to your backups. Refer to the following information for more details.

Instance operations that you can perform from Flex Appliance

Use Flex Appliance to do the following:

- Resize instance storage
- Edit instance network settings
- Assign or unassign Fibre Channel ports
- View instance performance metrics
- Upgrade application instances
- Manage application add-ons, including NetBackup EEBs
- Delete application instances
- Clear a configuration error status
- Manage remote replication
- Setting resource limits
- Network Access Control settings for the instance

See “Managing application instances from Flex Appliance” on page 85.

Instance operations that you can perform from NetBackup

Other management tasks happen from NetBackup. The *NetBackup Application Guides* cover the information that is specific to the NetBackup application. For all other tasks, refer to the regular NetBackup documentation as you would for any other environment.

Managing application instances from Flex Appliance

You can manage some aspects of your application instances from the **System topology** page of the Flex Appliance Console. To access your existing instances, click on the **System topology** box on the home page or the **System topology** icon in the left-side navigation bar, then navigate to the **Application instances** section.

Under **Application instances**, you can perform the following tasks, depending on the features that you have configured:

- Create a new instance.
  See "Creating application instances" on page 83.
- Create a replica.
  See "Creating a replica" on page 114.
- Use the Actions menu to the right of an instance to:
  - Relocate it to another node if you have a multi-node appliance.
  - Stop or start it.

    Note: When you start an instance, Flex Appliance automatically determines which node to start it on for optimal load balancing. Therefore, it may not start on the same node that it was located on when it was stopped. If you want the instance to run on a specific node, you can relocate it after it starts.

  - Delete it.
    See "Deleting an application instance" on page 98.
  - Resize the storage.
    See "Resizing instance storage" on page 86.
  - Upgrade it.
    See "Upgrading application instances" on page 99.
  - Install add-ons.
    See "Installing application add-ons" on page 95.

  - Clear a configuration error status.
    See “Clearing a configuration error status on an application instance” on page 98.
  - Pause or resume replication.
    See “Pausing and resuming replication” on page 118.
  - Change the replication role.
    See “Changing the replication role of an instance” on page 120.
  - Unlink it from its active or replica instance.
    See “Unlinking active and replica instances” on page 121.
- Click on an existing instance to:
  - View the instance details.
  - Edit the network settings, including IP address and interface pairs.
    See “Editing instance network settings” on page 87.
  - Manage add-ons.
    See “Managing application add-ons on instances” on page 94.
  - Manage the assigned Fibre Channel ports.
    See “Assigning Fibre Channel ports to an instance” on page 92.
    See “Unassigning Fibre Channel ports from an instance” on page 94.

You can also view performance metrics of all of the instances on your appliance from the **Home** page or the Flex Appliance Shell. See “Viewing performance metrics” on page 138.

Note: Flex Appliance does not support adding local directories or manually editing most files on application instances. If you create a local directory or manually edit a file and the instance is relocated or stopped for any reason, the changes are not maintained when the instance restarts.

However, if you must store a small amount of critical data on an instance, you can store it in the `/mnt/nblogs` directory. Note that this directory has 250GB of storage space that cannot be resized. If you use too much storage space, the instance may be affected.

See the *NetBackup Application Guides* for specific details.

Resizing instance storage

Use the following procedure to change the storage allocations on an existing application instance in Flex Appliance.

Note: If you have configured remote replication, you can only resize the active instance. The replica instance is automatically resized to match when you resume replication after the resize. Make sure that the paired appliance has enough available storage to resize the replica. If it does not, you cannot resume replication until you have freed up or added the required storage.

Note: The maximum size you can allocate to an MSDP volume depends on the appliance model, its drive capacity, and the MSDP pool limits in NetBackup. On a 5372 appliance with 20-TB drives, an MSDP pool of up to 2.4 PiB is supported. See *About MSDP capacity support and hardware requirements* section in the *NetBackup Deduplication Guide*.

To resize the instance storage

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to modify. If it is running, click **Actions** > **Stop**.
3. If the instance has a replica, check the **Data status** from the **Remote replication** page and make sure that it shows a status of **Consistent**. If it does not, wait for it to become consistent and then return to the **Application instances** section of the **System topology** page.
4. Click **Actions** > **Resize storage**.
5. Select the volume that you want to resize. Then enter the new allocation and click **Resize**.
6. Wait for the resize operation to complete. You can monitor the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

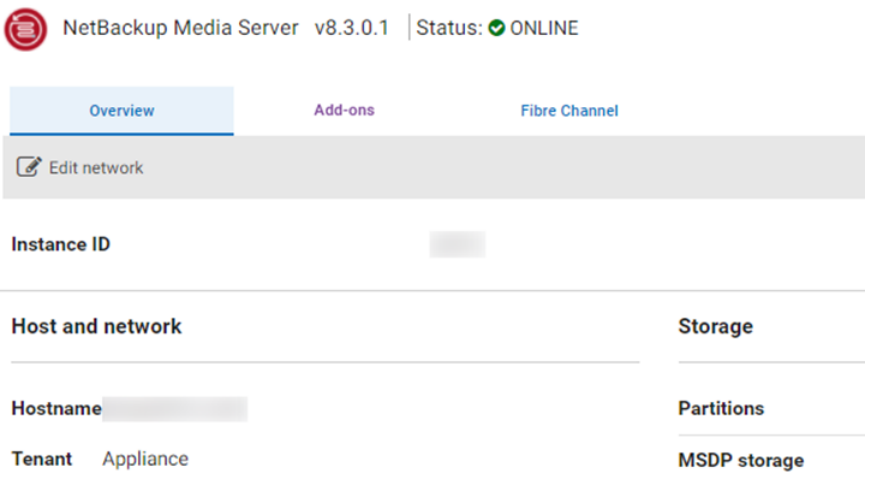
   When the resize is complete, you can view the new storage allocations by clicking on the instance name under **System topology** > **Application instances**.
7. If the instance has a replica, resume replication.

Editing instance network settings

Use the following procedure to edit the network settings of an existing application instance in Flex Appliance.

To edit the instance network settings

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to edit. If you want to edit the IP address and interface pairs or the default gateway, click **Actions** > **Stop**. You do not need to stop the instance to edit the other settings.
3. Click on the instance name to open the instance details page.



4. At the top of the details page, click **Edit network**.
5. Make the required changes. To add or remove IP address and interface pairs, click **Manage pairs**. To add or remove static routes, click **Manage routes**.

Note: If you change the protocol of the instance IP addresses, make sure that your configured NetBackup features support the new protocol. For example, if you have configured MSDP cloud on an instance and change the IP protocol to IPv6 only, the SSL setting **Check certificate revocation** must be disabled.

---

6. When you are done, click **Save**.
7. If you changed the IP address and interface pairs for the instance, make sure that you update your DNS configuration or add the new IP addresses to the `Hosts` file on all hosts that communicate with the instance. If the other hosts are application instances, you can add the new IP addresses to the `Hosts` file as follows:

- Follow the previous steps to edit the network of all application instances that need to communicate with the instance that you already edited. On the **Edit network** page, add the new IP addresses to the **Hosts file entries** field.
- Open an SSH session to each instance and run the following commands:
  - `sudo /usr/openv/netbackup/bin/bpclntcmd -clear_host_cache`
  - `sudo mv /usr/openv/var/host_cache /usr/openv/var/host_cache.old`
  - `sudo bp.kill_all`
  - `sudo bp.start_all`

Setting resource limits

You can set resource limits to allocate CPU and memory resources efficiently to ensure optimal application performance. It supports three tiers:

1. Best effort
   - Resources are shared with no guarantees.
   - No reservations are made for the instance. Resource availability depends on overall system load.
   - User Options: No option to set limits.
2. Burstable
   - Resources are available within a defined range but without strict guarantees.
   - Minimum resource value is reserved.
   - Maximum limit defaults to unlimited but can be modified by the user.
   - Applications may acquire resources beyond the minimum if available, but these can be reclaimed by the OS based on system needs.
   - User Options: Set minimum and optionally adjust maximum value.
3. Guaranteed
   - Resources are fully guaranteed.
   - Minimum and maximum limits are the same.
   - A fixed amount of resource is guaranteed at all times.
   - Applications cannot exceed the defined limit.
   - User Options: Set a single fixed limit.

Resource limits can be configured after the instance is created and can be modified at any time.

To set the resource limits

1. From the **System topology** page of the Flex Appliance console, go to **Application instances**.
2. Select the instance to open the detail page. Select the **Resource limits** tab.
3. Set the required CPU and memory limits.
   - CPU: Define the number of cores or CPU units allocated per instance (in millicores).
   - Memory: Specify the amount of RAM reserved for the instance (in MiB).

   It is recommended to use **Guaranteed** option for critical workloads requiring predictable performance. For flexible workloads, **Burstable** option offers a balance between efficiency and adaptability.

   Note: If the CPU or memory limits set for the instance are lower than what the application requires, its performance may degrade. Before applying resource limits, review the application's resource needs and verify the instance's actual usage on the dashboard for deeper insights. If you are unsure about the appropriate limits, choose **Best Effort**, where supported.
4. Click **Save**.

Network Access Control for application instances

Network access control is a security feature that restricts network access to services running inside application instances. By allowing access only through specified ports and an allowable IP/CIDR list, network access control minimizes attack exposure and ensures that only trusted sources can communicate with NetBackup instances. The network access control settings apply at the instance level and are enforced through firewall rules. The updated network access control details are saved in a dedicated network access control settings file for each instance. This ensures centralized management of network access control settings for each instance and controlled administration using role-based permissions.

Prerequisites:

- Appropriate role permissions for managing network access control settings.

You can assign network access control-related permissions when creating custom roles.

To create custom role with network access control-related permissions

1. Click the **Access management** icon in the left-side navigation bar to open the**Access management** page.
2. Go to the **Roles** page and click **Create role**.
3. In the **Create custom role** window:
   - Enter the role name and description.
   - Under Applications, select **Network access control**.
   - Select the required permissions.
4. Click **Review**.
5. In the **Permissions for the role** popup, review the permissions and click **Create**.

Use the following procedure to configure network access control for a service.

To configure network access control for services

1. From the **System topology** page of the Flex Appliance console, go to **Application instances**.
2. Select the instance to open the detail page. Select the **Network access control** tab.
3. Click **Add service**.
4. In the **Add service** window, enter the required details:
   - Service name: Enter the name of the service.
   - Ports and protocols: Enter ports or ports and protocols in a comma-separated list.
     Use `port/protocol` format (for example: 443/tcp).
     Supported protocols: tcp (default) and udp.
     Click **Add**.

     Note: Ports and protocols cannot be updated after the service is added.

   - Allowed list: Enter IP addresses or subnets in a comma-separated list. Click **Add**.
   - Description: (Optional) Provide a brief description.
5. Click **Add**.

The instance details page will list the newly added service.

You can edit or delete the service by selecting the service and navigating to **Action > Edit** or **Action > Remove**.

Note that:

- If network access control settings fail during instance startup, an SMTP/SNMP alert is generated to notify administrators.
- The network access control rules apply only to inward network traffic to application instances.
- Select **Enable network access control** if you want to apply the firewall settings to the instance. Unselect this option when you want to clear the firewall settings.
- If you configure network access control on an application in which IRE is also configured, a combination of firewall rules from both the settings will be applied.
- The Instance details page displays the firewall table rules currently applied to the instance.
  Click **View details** next to **Live firewall settings** to review the configuration and identify the network access control settings file.
- You can find the logs at `/var/log/application/instance-nac-<instance-id>.log` if the connection is rejected by network access control.
- If the WORM instance version is 21.1.0.2 and later and if the primary and media server version are 11.1.0.2 and later, the default services to which you can add network access control are listed in the **Network access control** tab

Assigning Fibre Channel ports to an instance

To perform backups over Fibre Channel, you must assign ports to your application instances.

This release supports the following types of backups over Fibre Channel:

- VMware SAN transport (initiator)
- Tape out (initiator)
- SAN client (Fibre Transport target)

Use the following procedure to assign one or more Fibre Channel ports to an application instance.

To assign Fibre Channel ports to an instance

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to assign ports to. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page, then navigate to the **Fibre Channel** tab.
4. Click **Assign ports** and follow the prompts to assign available ports.

   If you assign a port as an initiator that was previously used as a target, you are prompted to scan the port before you can continue.

Note: Depending on the use case you select for the port, only the devices of that storage type are visible to the instance. If you want all devices to be visible to the instance, select all available options from the **Used for** drop-down menu.

Port sharing and multipathing support

Note the following information:

- You can assign an initiator port to multiple instances if the instances belong to the same tenant. You cannot assign a target port to multiple instances.
- You can use the same port for both VMware and Tape out backups.
- You can assign multiple ports to the same application instance or instances as long as they meet the following guidelines:
  - Used for VMware SAN transport:
    Multiple ports can be assigned to a single or to multiple application instances in any combination.
  - Used for Tape out or for both Tape out and VMware SAN transport:
    Multiple ports can be assigned to a single or to multiple application instances. However, the ports that are connected to the same tape devices must also be connected to the same application instances. The same tape devices cannot be assigned to different instances using different ports.
  - Used for SAN client:
    Multiple ports can be assigned to a single or to multiple application instances in any combination. Once you have assigned the ports, you cannot assign them to additional application instances or use them for another use case unless you unassign the existing instances.

  - Assigned to load balancing servers:
    If you have configured multiple media server instances as load balancing servers and want to use Fibre Channel for VMware SAN transport, you must assign the same ports to all of the load balancing media server instances.

- A Fibre Transport (FT) target port can handle data streams from multiple SAN client initiator ports concurrently. However, if you want it to handle streams from more than two SAN client initiator ports, consider changing the following NetBackup primary server setting:

  ```
  nbftconfig -setconfig -ncp4
  ```

  Caution: This setting applies to all FT target ports on all media servers in your NetBackup domain. This setting should only be increased from the default (2) when all of the following conditions exist:

  All FT target ports on all media servers are at least eight gBit/s link speeds.

  The mix of jobs is such that all of the media servers have unused FT pipes.

  A large number of jobs from other SAN clients are waiting for resources.

  The back-end storage units have a lot of unused throughput capacity.

  If you increase the `-ncp` setting too high, the load balancing between multiple FT media servers could become highly imbalanced.

Unassigning Fibre Channel ports from an instance

Use the following procedure to unassign Fibre Channel ports from an application instance.

To unassign Fibre Channel ports from an instance

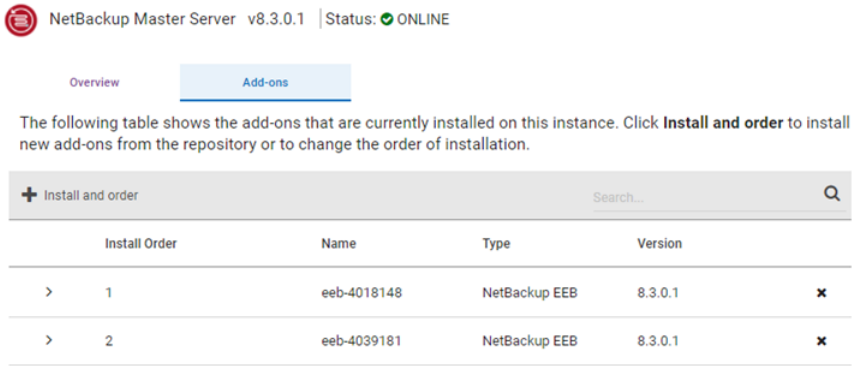
1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to unassign ports from. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page, then navigate to the **Fibre Channel** tab.
4. Select the port or ports that you want to unassign and click **Unassign ports**.

Managing application add-ons on instances

Flex Appliance instances support the following types of add-ons:

- NetBackup emergency engineering binaries (EEBs)
- NetBackup EEB packages
- Cohesity-provided plug-ins
- OpenStorage (OST) plug-ins

You can view and manage the add-ons on an instance from the **Application instances** section of the **System topology** page. Click on the instance name to open the instance details page, then navigate to the **Add-ons** tab. From there, you can view the currently installed add-ons and make changes.



You can also use the Actions menu in the **Application instances** section to install and order add-ons on the instance.

See “Installing application add-ons” on page 95.

See “Uninstalling application add-ons” on page 96.

See “Changing the application add-on installation order” on page 97.

Installing application add-ons

Use the following procedure to install an add-on on an instance.

To install add-ons

1. Make sure that the add-ons you want to install are located in the repository. See “Managing the repository” on page 80.
2. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
3. Locate the instance on which you want to install the add-ons. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.

4. Click **Actions** > **Install add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.
5. Select the appropriate add-ons from the repository list that appears. When you are done, click **Next**.
6. On the following page, you have the option to change the add-on installation order. In most cases, the install order does not affect operation, and you can skip this step. However, if recommended by Support or otherwise required, you can use the up and down arrows to change the order.

   If any of the add-ons have conflicting changes, alert messages appear to let you know of the conflicts and the resulting actions. Click **View report** at the top of the page for more detailed information. If you agree with the default resolution, proceed to the next step.

   Otherwise, resolve the conflicts manually as follows:

   - If a conflict exists between new add-ons, the add-on that is listed last takes precedence. You can use the up and down arrows to change the order and prioritize a different add-on.
   - If a conflict exists between a new add-on and an installed add-on, the new add-on is not installed. If you want to install the new-add-on, click **Cancel** to back out of the procedure. Then remove the installed add-on and try again.
   - If a conflict exists between installed add-ons, you must remove one of the add-ons before you can continue. Click **Cancel** to back out of the procedure.
   - If all of the add-ons are required or if you are unsure which add-ons should be installed, contact Support for assistance. Before you do so, navigate to the **Conflict report** and click **Copy**. Share this report with your representative.
7. Click **Install**.

Note: If the instance that you installed the add-ons on has a replica, make sure that the remote administrator also installs them on the replica. Alternatively, you can make sure the add-ons are in the repository on the remote appliance and then pause and resume replication.

Uninstalling application add-ons

Use the following procedure to uninstall an add-on from an instance.

To uninstall an add-on

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance from which you want to uninstall the add-on. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click on the instance name to open the instance details page.
4. At the top of the details page, navigate to the **Add-ons** tab.
5. Click the **X** icon next to the add-on that you want to uninstall.

Changing the application add-on installation order

In most cases, the order in which add-ons are installed on an instance does not affect operation. However, if recommended by Support or otherwise required, use the following procedure to change the order.

To change the add-on install order

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the instance that you want to modify. If it is running, click **Actions** > **Stop**. You can also wait to stop the instance until the Flex Appliance Console prompts you to if you prefer.
3. Click **Actions** > **Install add-ons**. Alternatively, click on the instance name, navigate to the **Add-ons** tab, and click **Install and order**.
4. In the wizard that appears, click **Next** to skip the add-on installation step.
5. Use the up and down arrows to change the add-on install order as needed.
6. Click **Install**.

Updating an application add-on to a newer revision

Periodically, new revisions of application add-ons are released to address security updates. When a new revision is released, it is posted on the Download Center with a new file name that includes the revision number after the version.

For example, the file `VRTSflex-nb_EEB_ET4070421-10.0-9.x86_64.rpm` indicates that the version is 10.0, and the revision number is 9.

You can view the revision numbers of your add-ons on the **Application add-ons** page of the **Repository**.

Use the following procedure to update an application add-on to a newer revision.

To update an add-on to a newer revision

1 Add the new revision of the add-on to the repository.

Note: If the instance that has the add-on installed has a replica, make sure that the new revision is also in the repository on the remote appliance.

See "Adding files to the repository" on page 81.

2 Restart the instance that has the add-on installed.

Note: If you have more than one instance that has the add-on installed, they all get updated to the newer revision the next time they are restarted or if you change the replication role for remote replication.

Clearing a configuration error status on an application instance

If a configuration error occurs when you create or upgrade an application instance, the **Application instances** section shows one of the following error statuses:

- Instance creation error: **ONLINE | Configuration Failed**
- Instance upgrade error: **<*Version*> (upgrade failed)**

If you see one of these errors, use the following procedure to clear the error status.

To clear a configuration error status:

1 Before you can clear the error status, you must resolve the underlying configuration error or errors. Hover over the **Configuration Failed** status to see more specific information, and refer to the error messages that display in the Activity Monitor. Then log in to the instance and resolve all errors.

2 When you are sure that all errors have been resolved, navigate to the **System topology** > **Application instances** section.

3 Locate the instance and click **Actions** > **Clear status**, then refresh the page to see the change.

Deleting an application instance

Use the following procedure to delete an application instance.

To delete an application instance

1 Deleting an application instance requires multiperson authorization for the following versions:

- NetBackup primary or media server instances on version 10.3.0.1 or later
- NetBackup WORM storage server instances on version 19.0.1 or later
- NetBackup WORM storage server instances on version 19.0 in the following scenarios:
  - The appliance is in compliance lockdown mode.
  - The appliance is in enterprise lockdown mode, and you do not have the security administrator role.

With multiperson authorization, the application administrator must unlock the deletion option before you can delete the instance. Ask them to refer to the topics “Authorizing a primary or a media server instance for deletion” and “Authorizing a WORM storage server for deletion” in the *NetBackup Application Guide*.

2. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
3. Locate the instance that you want to delete and click **Actions** > **Delete**.

Note: Depending on the application type and version and the lockdown mode of the appliance, the instance may need to be running before you can delete it. If the instance is stopped, and you don’t see the **Delete** option, start it and try again.

Upgrading application instances

Use the following procedure to upgrade an existing instance in Flex Appliance.

Note: If you plan to update Flex Appliance and upgrade your application instances at the same time, update the appliance first. During this process, you may temporarily run an earlier, unsupported version of NetBackup on the updated appliance, until you can upgrade the instances. Cohesity recommends that no backups, duplications, replications, or other activities take place on the system until all NetBackup instances have been upgraded to a supported version.

To upgrade an instance

1. Make sure that the new version of the application is located in the repository. See "Managing the repository" on page 80.

   Note: If the instance that you want to upgrade has a replica, make sure that the new version of the application is also located in the repository on the paired appliance.

   ---

2. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
3. Locate the instance that you want to upgrade. If it is stopped, click **Actions** > **Start** before you begin the upgrade so that the upgrade precheck can run.
4. Stop all current backup operations on the instance.
5. From the **Application instances** section, click **Actions** > **Upgrade instance**.
6. Select the version that you want to upgrade to and click **Precheck**.
7. If the precheck passes, click **Next** to continue. If the application needs any additional configuration parameters, you are prompted to enter them. Enter the parameters and click **Next**. Then verify the selection summary and click **Upgrade** to begin the upgrade process.

   If the precheck returns with any error messages, resolve the issues before continuing with the upgrade.

   If the upgrade fails for any reason, the instance automatically rolls back to the previous version. You can find more detailed information on the failure in the Activity Monitor. Resolve any issues before restarting the upgrade procedure.
8. If your application does not support rollback, the upgrade is now complete.

   If your application does support rollback, the instance version remains in a pending state for the next 24 hours. You must decide within that time period whether you want to commit to the new version or roll back to the previous version. Note that some operations are restricted until you commit or roll back. Complete the rest of this procedure to restore full functionality.

   Warning: Performing a rollback may lead to inconsistencies between the NetBackup catalog and the media servers for all jobs that ran after the upgrade. These inconsistencies can affect future backups.

   See "Warnings and considerations for instance rollbacks" on page 101.

To commit or roll back the instance version, navigate to the **System topology** > **Application instances** section and do one of the following:

- To commit to the new version, locate the instance and click **Actions** > **Upgrade instance** > **Commit**. You can also click on the instance name to open the instance details page, then click **Commit** at the top of the screen.
- To roll back to the previous version, stop all current backup operations on the instance. Then locate the instance and click **Actions** > **Upgrade instance** > **Roll back**. You can also click on the instance name to open the instance details page, then click **Roll back** at the top of the screen.

Warning: Before you roll back the version of a primary server instance, check the versions of all media servers and clients that are used with it. The version of the primary server after rollback must be equal to or later than the versions of the connected hosts, including media server instances.

Caution: If you do not commit or roll back within 24 hours of the upgrade, the new instance version is committed automatically.

Warnings and considerations for instance rollbacks

If you need to roll back an instance upgrade, review the following information before you begin.

- Instances with MSDP storage do not support rollback. If you experience an upgrade failure that you cannot resolve, contact Technical Support for assistance.
- Rollback of other instances should only be attempted as a last resort if there were serious problems with the upgrade.
- A rollback restores the instance to a pre-upgrade checkpoint and reverses all operations that were performed after the upgrade, including backup data. For this reason, backup operations should be kept at a minimum for testing purposes only while the instance upgrade is in a pending state. Do not perform production operations until you commit or roll back the upgrade.
- You cannot resize the instance storage until you commit or roll back the upgrade.
- If you upgrade and roll back an application instance that has a lot of configured storage, the rollback can take a long time to complete. For example, an instance with 1 Petabyte of storage can take a little over an hour to roll back.

- If a rollback is performed, there is a risk of data loss and data leakage for all operations that are performed after the upgrade. The longer the system was up and running before a rollback, the greater the chance of data loss and leakage. The data loss is not limited to losing backup data for the jobs that ran before the rollback. Future backups can be affected as well.
  The following inconsistencies can occur if you decide to roll back:
  - Incremental or transaction log-based database backups:
    If transaction logs were truncated after the upgrade and before the rollback, the database may not be protected.
    To resolve this issue, perform a full database backup after the rollback.
  - Incremental Windows file system backups:
    If the archive bit is used for incremental backup, it is reset upon completion of an incremental backup. If a rollback occurs, the incremental backup is lost, and subsequent incremental backups do not detect that these files changed. The files are not backed up again until a full backup is performed.
    To resolve this issue, perform a full backup after the rollback. If any files were modified in the lost incremental and then deleted before the next full backup, those files are lost.
  - Backup expiration catalog and storage inconsistency:
    If backup images expire and cleanup begins after the upgrade and before the rollback, backup data may be removed from storage units external to the instance. For example, this behavior can happen with an MSDP media server, cloud storage, OST storage, or tape storage. When a rollback of the primary server catalog occurs, the catalog indicates that there is a valid backup even though the data was removed from storage. This inconsistency results in backup data that cannot be restored, duplicated, or replicated. It may also affect scheduling of subsequent backups (delaying backups or performing incrementals instead of fulls).
  - Orphaned backups on storage:
    If backup images are created on external storage after the upgrade and before the rollback of the primary server, the backup images exist on storage but not in the NetBackup catalog. This discrepancy results in situations where the backups are never removed from storage (data leakage).
    To resolve this issue, import the images from storage or use the consistency check tools.
  - Backup considerations if the instance is a media server:
    - The backups between the upgrade and rollback are not restorable even though NetBackup has them in the catalog.

- Unfinished SLP jobs fail, causing inconsistencies between the NetBackup primary server and the storage.
  If any backups were deleted after the upgrade and before the rollback, those backups come back as storage leak.

Updating an application instance to a newer revision

Periodically, new revisions of applications are released to address security updates. When a new revision is released, it is posted on the Download Center with a new file name that includes the revision number after the version.

For example, the file `VRTSflex-netbackup-9.1.0.1-0043x86_64.rpm` indicates that the application version is 9.1.0.1, and the revision number is 0043.

You can see the revision number of uploaded applications on the **Repository** page for NetBackup 10.3 revision 67 and later. Earlier versions do not show the revision numbers.

Use the following procedure to update an application instance to a newer revision.

Note: The Flex Appliance Console does not currently show the revision numbers of your application instances. To determine the current revision of an instance, log in to the Flex Appliance Shell and run the following commands:

```
support shell
```

```
docker inspect flex.io/netbackup/main:<version> --format='{{index
.Config.Labels "image.revision"'}}
```

Where *<version>* is the version number of the application instance.

To update an instance to a newer revision

1 Add the new revision of the application to the repository.

Note: If the instance that you are updating has a replica, make sure that the new revision is also in the repository on the remote appliance.

See "Adding files to the repository" on page 81.

2 Restart the instance.

Note: If you have more than one instance of the application, they all get updated to the newer revision the next time they are restarted or if you change the replication role for remote replication.

About Flex Appliance updates

Flex Appliance provides product enhancements and fixes with the following types of releases:

- Software updates
  A software update contains new features, enhancements, and fixes for Flex Appliance. It modifies the operating system, the appliance interfaces, or both.
- Firmware updates
  A firmware update modifies the firmware on the appliance hardware components, including the BIOS, storage, network interface cards, and Fibre Channel ports. The version number for a firmware update is not related to the Flex Appliance version.

Cohesity recommends that you install updates when available to make sure that you have the latest product features and fixes.

Updating Flex Appliance

A node update can be done in two ways.

- Select the **Prepare and Apply Update** option to do a single step update. Applications on the node must be offline during the update process.
- Select the **Prepare Update** option followed by the **Apply Update** option to do a two-step update. Applications can continue to run on the node during **Prepare Update** step but applications must be offline during the **Apply Update** process. The advantage of this option is that in a multi-node cluster, prechecks and

Prepare Update can run in parallel on both the nodes, minimizing downtime and giving you greater control and flexibility when you make updates.

Note: The two-step update option is supported only for upgrades from version 7.0 and later.

Use the following procedure to update the Flex Appliance software from version 7.0 to a later release.

Note: To update to version 7.0, refer to the *Getting Started and Administration Guide* for the version that you are currently on.

Before you begin the update, note the following information:

- If you plan to update Flex Appliance and upgrade your application instances at the same time, update the appliance first. During this process, you may temporarily run an earlier, unsupported version of NetBackup on the updated appliance, until you can upgrade the instances. Cohesity recommends that no backups, duplications, replications, or other activities take place on the system until all NetBackup instances have been upgraded to a supported version.
- **If you have remote replication configured, note the following:**
  - Make sure that there is no data lag before you begin.
  - Update the appliance with the active instances first. If both appliances have active instances, pick any one to start with. Once the update is committed on the first appliance, update the second appliance.
  - Simultaneous updates on both sites are not supported.
  - When an update starts on a site, only that appliance enters maintenance mode. The remote appliance remains operational and displays a maintenance notification for the peer appliance.
    After the appliance commit or rollback is complete, the appliance exits maintenance mode and the notification is cleared on the peer appliance.
  - Flex Appliances running different software versions can continue replication until both sites are updated to the same version.
  - If replication is manually paused prior to the upgrade, it must be manually resumed only after both the upgrade and the commit operations are fully completed. Replication cannot be resumed until these processes are complete.

- If more than the tested number of Fibre Channel devices or paths are connected to the appliance, Cohesity recommends that you disable the ports or disconnect the devices before you begin this procedure. When the procedure is complete, reenable or reconnect them. You may need to scan the ports from the Fibre Channel interfaces page.

See "Managing the appliance Fibre Channel ports" on page 41.

To update Flex Appliance

1. On the Flex Appliance Console, click the **Repository** icon in the left-side navigation bar and navigate to the **Appliance updates** tab.
2. Make sure that the update package you want to use is located in the repository. Before you can add a Flex Appliance update package, you must first download it from the Downloads page on the Support website. See "Managing the repository" on page 80.
3. Run a precheck on each node.

   To run the precheck, select the node or nodes and click **Run precheck**. If you have a multi-node appliance, you can run the precheck simultaneously on both the nodes.

   You can view the status of the precheck in the **Progress status** column. After the precheck is complete, the **Progress status** changes to `Ready for Prepare Update`.

   Click on the **Precheck status report** link corresponding to each node if you want to view the details. If the precheck reports any issues, correct them and re-run the precheck before you proceed with the update.

   You have the option to fix only the prechecks related to the **Prepare Update** step if you plan to run **Prepare Update** first. Based on which precheck categories pass, the UI will present only the operations that are supported and available for you to perform.
4. Select the node that you want to update.
   - If you want to do a one step update:
     - If you have a single-node appliance, stop all running instances.
     - If you have a multi-node appliance, stop all running instances or select the node that you want to update first and relocate all of its instances to the other node.

     Note: You cannot update both nodes simultaneously.

- Click **Prepare and Apply Update**.

- If you want to do a two-step update:
  - Select the nodes that you want to prepare and click **Prepare Update**. This step can be done on both the nodes simultaneously.
  - Wait for the **Prepare Update** process to complete. The **Progress status** changes to `Ready for Apply Update` after the update is prepared.
  - If you have a single-node appliance, stop all running instances.
  - If you have a multi-node appliance, stop all running instances or select the node that you want to update first and relocate all of its instances to the other node.
  - Click **Apply Update**.

Note: If the update-related prechecks did not pass, the **Apply Update** button will not appear, and you will need to rerun the prechecks and ensure they pass before continuing.

Use the **Activity monitor** to track the status of the tasks.

5 If the update requires a restart, you can monitor the restart progress from the Veritas Remote Management Interface. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 22.

Warning: Do not make configuration changes, start application instances, or restart the appliance while the update is in progress.

---

6 When the update process is done, refresh your browser cache and sign back in to the Flex Appliance Console.

7 If you have a multi-node appliance, make sure that the update completed successfully on the first node. Then stop or relocate all instances on the other node and repeat the update on that node.

Do not attempt to update the second node if the update failed on the first node.

8 If the update release that you installed supports rollback, you must decide whether you want to commit the new version or roll back to the previous version.

Some operations are restricted until you commit or roll back, or if the nodes are running different software versions. Update both nodes and complete the rest of this procedure to restore full functionality.

Warning: If you change any passwords during this time, make sure that the old passwords are saved in a secure location. If you roll back, the password changes are reversed. If you installed any add-ons, they are also removed during the rollback.

Do one of the following:

- To commit the update, return to the **Appliance updates** tab on the **Repository** page and click **Commit**.
  The **Commit** option is also available in the notification banner.
- To roll back to the previous version, stop all instances on the appliance and then run the following command from the Flex Appliance Shell:
  ```
  system rollback
  ```
  Restart the node when prompted. If you have a multi-node appliance, you must run this command on all nodes.

  Warning: If you have a multi-node appliance, you must roll back all nodes before you perform any other operations, including retrying an update. Complete the rollback and restart on the first node before you proceed with the next node. Do not remove the update RPM from the repository until the rollback is fully complete.

9 If you rolled back, refresh your browser cache before you sign back in to the Flex Appliance Console.

10 After you complete the software update, also make sure that the appliance firmware is up to date. See “Updating the firmware” on page 108.

Updating the firmware

Use the following procedure to update the appliance firmware.

If you make any hardware changes after you install a firmware update, make sure that you install the update again for the new hardware.

You can check the supported firmware for your hardware model from the Appliance Compatibility List.

Use the appliance firmware update tool to get the latest firmware update RPMs.

To update the firmware

1. On the Flex Appliance Console, click the **Repository** icon in the left-side navigation bar and navigate to the **Appliance updates** tab.
2. Make sure that the update package you want to use is located in the repository. See "Managing the repository" on page 80.
3. Navigate to **System topology** > **Application instances** to check the status of the application instances.
4. Do one of the following:
   - If you have a single-node appliance, stop all running instances.
   - If you have a multi-node appliance, stop all running instances or select the node that you want to update first and relocate all of its instances to the other node.
5. Return to the **Appliance updates** tab on the **Repository** page. Select the node that you want to update and click one of the following:
   - To install the firmware update for the first time, click **Update**.
   - To install the firmware update again because of new hardware, click **Update again**.

   If your appliance model supports BIOS password protection and has a non-default password, you are prompted for the BIOS password.

   If the update requires a restart, you can monitor the restart progress from the Veritas Remote Management Interface. However, the interface briefly becomes unavailable during the update. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 22.

   Warning: Do not start any application instances while the update is in progress.

   ---

6. When the update process is done, refresh your browser cache and sign back in to the Flex Appliance Console.
7. If you have a multi-node appliance, stop or relocate all instances on the other node.

   Then repeat the update on the other node.

Changing the BIOS password

If you have a 5260 or a 5360 appliance, Cohesity recommends that you change the BIOS password. The other appliance models do not support BIOS password protection.

You can see the last time that the password was changed from the **System topology** page.

Use the following procedure to change the BIOS password on a 5260 or 5360 appliance.

To change the BIOS password

1. Sign in to the Flex Appliance Console as a BIOS administrator and navigate to the **System topology** page.
2. In the **Head nodes** widget, locate the node that you want to change the password of. Click **Change password**.
3. Follow the prompts to enter a new password.

   If you have never changed the password before, the default password is the node's serial number.

   BIOS password policy:

   Note: The new password must be different from the current password.

   - Minimum length: 8
   - Maximum length: 14
   - Minimum numbers: 1
   - Minimum lowercase characters: 1
   - Minimum uppercase characters: 1
   - Minimum special characters: 1
   - Allowed special characters (new password): @ # % ^ * ( ) - _ + = ?
   - Allowed special characters (current password): ! @ # $ % ^ & * ( ) - _ + = ?
   - Maximum consecutive repeating characters: 3
   - Maximum consecutive repeating characters of same type: 4

Note: The characters !, &, and $ are accepted in the current password field but are not valid for the new password.

Warning: The BIOS password cannot be recovered. Clearing the password requires using the system board jumper (password reset jumper). Ensure that you store the password in a secure location before setting it.

Locating the node serial number

The node serial number is required for some operations on the appliance. You can find the node serial number in the following locations:

- On the **System topology** page of the Flex Appliance Console, under **Head nodes**.
- With the following command in the Flex Appliance Shell:
  ```
  show serial-number
  ```
- On the **System** > **FRU Information** page of the Veritas Remote Management Interface, under **Product Information**
- On the hardware. For the exact location, see the *Product Description* for your particular appliance.

Chapter 7

Remote replication

This chapter includes the following topics:

About remote replication

Remote replication saves replicas of your primary server application instances on another appliance. You can use remote replication to minimize downtime during planned maintenance or troubleshooting activities and as additional protection from a disaster scenario. You can also use remote replication to easily migrate your data from one Flex appliance to another.

Note: Remote replication is not an alternative to the NetBackup catalog backup policy. You should still configure a NetBackup catalog backup policy on your primary server. See the topic "Mounting an NFS share on a NetBackup primary server instance" in the *NetBackup Application Guide* for details.

To configure remote replication, you need two Flex appliances. An administrator from each appliance must coordinate to pair the appliances, and then you can create replicas of your primary server instances.

See “Pairing appliances for remote replication” on page 113.

See “Creating a replica” on page 114.

Pairing appliances for remote replication

Use the following procedures to pair two appliances for remote replication. These steps require the coordination of an administrator from each appliance. You can start pairing from either appliance.

Prerequisites

Make sure that the following prerequisites are met before you begin.

- The node IP addresses of each appliance must be able to communicate with the console IP address of the other appliance.
- If you use network access control, make sure that each appliance's allowed list includes all node IP addresses of the other appliance.
- You must have a network interface configured to use for replication. Cohesity recommends that you do not select a shared interface or an interface that is configured with the same subnet as the appliance node IP addresses.
- The following ports must be open in both directions between the two appliances:

  Between the replication IP addresses:

  - 4145 (TCP and UDP)
  - 8199 (TCP and UDP)
  - 8989 (TCP and UDP)

  Note: If you need to use the same subnet for replication and the node IP addresses, these ports must also be open between each appliance's replication IP address and the other appliance's node IP addresses.

  Between all of the node and the Flex Appliance Console IP addresses:

  - 443 (TCP)

Step 1: First appliance sends a fingerprint

To start the pairing process, the administrator of one of the appliances must send a client fingerprint to the second administrator. Use the following steps.

To send the fingerprint

1. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
2. Click **Copy fingerprint**.
3. Share this fingerprint securely with the administrator of the second appliance.

Step 2: Second appliance starts pairing

Once the second administrator has the fingerprint from the first appliance, they can start pairing. Use the following steps.

To start pairing

1. Obtain the fingerprint from the first appliance administrator.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Start pairing**.
4. Follow the prompts to enter the fingerprint and configure the network for replication.

   If you select an interface that was configured with a dual stack IPv4-IPv6 network, you can only use one of the protocols for the replication IP address.
5. When the pairing key displays, copy the key and share it securely with the first administrator.

Step 3: First appliance finishes pairing

Once the first administrator has the pairing key, they can finish pairing. Use the following steps.

To finish pairing

1. Obtain the pairing key from the second appliance administrator.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Finish pairing**.
4. Follow the prompts to enter the pairing key and configure the network for replication.

   When you are done, you can monitor the progress in the Activity Monitor on both appliances. Once the pairing has completed successfully, the **Paired appliances** section of the **Remote replication** page shows the **Management connection status** and the **Replication connection status** as **Connected**.

Creating a replica

Once you have paired two appliances, you can create replicas of your primary server application instances on either appliance.

Note: The appliance where you create the replica must have enough available storage to accommodate the size of the instance. Both appliances also require up to an extra 20% of the size of the instance to be reserved for replication logging.

Use the following procedure to create a replica.

To create a replica

1. Sign in to the Flex Appliance Console on the appliance that you want to create the replica on.
2. Click the **Remote replication** icon in the left-side navigation bar, then click **Create replica**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page and click **Create** > **Create replica**.
3. Locate the instance that you want to create a replica of.

   If any prerequisites are not met for that instance, it is greyed out, and the **Status** column shows **Missing prerequisites**. Click **Missing prerequisites** to see the list of issues. You must resolve them before you can continue.
4. Select the instance and click **Next**.
5. Follow the prompts to create the replica. When you are done, the replica appears on the **Remote replication** page with a status of **Configuring**. You can view the progress in the Activity Monitor.

   Once the replica has been created, the **Remote replication** page on the remote appliance updates as well. The instance that you created the replica of displays on this page as an active instance.

   Note: The instance widgets on the **Remote replication** page have different available actions, depending on whether they are for the active or the replica instance.

Managing remote replication

Once you have paired two appliances, you can manage the pairing and your replicas from the following locations:

- The **Remote replication** page

  From this page, you can edit the replication network, create and manage replicas, and monitor your configuration.
- The **Home** page

This page includes a **Remote replication** widget that alerts you to any issues with the replication network, the management network, or your replicas.

- The **System topology** page
  From this page, you can use the **Application instances** section to create and manage replicas.

Remote replication best practices

When you configure remote replication, Cohesity recommends that you adhere to the following best practices:

- When you configure remote replication for the first time, start with one replica per appliance. Then monitor the replication performance. Based on the results, you can consider creating additional replicas.
- Use a dedicated network for replication.
- If you configure remote replication on a 52xx appliance without storage shelves, use that appliance for primary server instances only. If you want to add media and WORM instances, add storage shelves with enough storage capacity to handle them.
- Configure email alerts to make sure that you are notified of any issues with the replication.

Monitoring remote replication

You can monitor remote replication from the **Remote replication** page. This page provides information about the network between your paired appliances, and individual widgets display the status of all active and replica instances on the appliance.

If an issue occurs with replication, the Flex Appliance Console may alert you in the following ways:

- An alert message appears in the **Remote replication** widget on the **Home** page.
- An alert icon appears next to the **Remote replication** icon in the left-side navigation bar.
- The connection status changes in the **Paired appliances** section of the **Remote replication** page. It turns yellow if the connection is degraded or changes to **Disconnected** if the connection is lost.
- If you have email alerts configured, an email alert is sent.

Editing the replication network

Use the following procedure to edit the replication network between two paired appliances. The replication connection status must be **Connected** to edit the network, and the old and the new IP addresses must have a network connection to each other.

Note: You cannot change the protocol (IPv4 or IPv6) of the network.

Use the following procedure to edit the replication network.

To edit the replication network

1. From the Flex Appliance Console on the appliance that you want to edit the network of, pause replication. See “Pausing and resuming replication” on page 118.
2. Navigate to the **Remote replication** page. Under **Paired appliances**, click **Edit network interface**.
3. Change the network details as needed and click **Save**.
4. Resume replication.

Repairing a lost connection between paired appliances

If your paired appliances become disconnected, first check if either of the appliances is under maintenance (for example, an appliance update or a factory reset). If so, wait for the maintenance to complete and recheck the status. In some scenarios, the connection repairs itself after the maintenance is complete.

If neither appliance is under maintenance or if the maintenance is complete, but the connection status still shows as **Disconnected** with a **Repair connection** option, use the following procedures to repair the connection. These steps require the coordination of an administrator from each appliance.

Steps for the administrator on the first appliance

The administrator of one of the appliances must start the repairing process.

To start repairing

1. Obtain the fingerprint of the second appliance from the second appliance administrator. To locate the fingerprint, the second administrator can navigate to the **Remote replication** page and click **Repair connection**. The fingerprint displays at the bottom of the window that appears. Make sure that they share it with you in a secure manner.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Repair connection** > **Start repairing**.
4. Enter the fingerprint. When the repairing key displays, copy the key and share it securely with the second administrator.

Steps for the administrator on the second appliance

The administrator of the second appliance must finish the repairing process.

To finish repairing

1. Obtain the repairing key from the first administrator.
2. From the Flex Appliance Console on your appliance, navigate to the **Remote replication** page.
3. Click **Repair connection** > **Finish repairing**.
4. Enter the repairing key and click **Save and close**. Note that the repair can take up to 15 minutes to complete.

Pausing and resuming replication

Use the following procedures to pause or resume replication between an active and a replica instance. The replication connection status must be **Connected** to pause or resume replication.

Warning: If you pause replication, the data between the active and the replica instances becomes out of sync. The longer that replication is paused, the longer it takes for the data to sync again when you resume. Only pause replication when it is specifically required for maintenance activities on the instances or the appliances.

To pause replication

1. Sign in to the Flex Appliance Console on either appliance.
2. Navigate to the **Remote replication** page and locate the instance that you want to pause. Under **Replication status**, click **Pause**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page. Locate the instance that you want to pause and click **Actions** > **Pause**.

To resume replication

1. Sign in to the Flex Appliance Console on the appliance where the active instance is located.
2. Navigate to the **Remote replication** page and locate the instance that you want to resume. Under **Replication status**, click **Resume replication**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page. Locate the instance that you want to resume and click **Actions** > **Resume replication**.

   You are redirected to the Activity Monitor to view the progress.

Note: As part of the resume operation, the appliance checks for the following configuration changes on the active instance: an instance upgrade or update, add-on installations or updates, and storage resizes. It attempts to make the same changes on the replica. Once those changes have been made on the replica, replication resumes.

Resolving discrepancies between an active and a replica instance

An active instance and its replica instance should always have the same configuration. However, discrepancies can occur between them in the following scenarios:

- You upgrade or update the active instance, but the newer version or revision is not in the repository on the appliance where the replica is located.
- You install a new add-on on the active instance but do not install it on the replica instance.
- You update an add-on on the active instance, but the newer revision is not in the repository on the appliance where the replica is located.
- You update the replica instance to a newer revision.
- You install or update an add-on on the replica instance

To avoid these scenarios, adhere to the following best practices:

- Always make sure that the required application and add-ons are available in the repositories on both appliances.
- If you install an add-on on the active instance, also install it on the replica instance. Alternatively, you can make sure the add-on is in the repository on the appliance where the replica is located and then pause and resume replication.
- Do not perform operations on the replica instance unless they are required to match the configuration of the active instance.

You can verify the configurations of the active and the replica instances from the **Remote replication** page. Locate the instance that you want to check and click **Compare configurations**. The window that appears displays discrepancies if any exist, along with instructions on how to resolve them.

Changing the replication role of an instance

You can change the replication role of an instance so that the active instance becomes the replica, and the replica becomes the active instance. You can use this option during planned downtimes on the appliance with the active instance so that the primary server can continue to run.

Use the following procedure to change the replication role. The replication network must be connected, and the data status between the instances must be consistent before you begin.

To change the replication role

1. Sign in to the Flex Appliance Console on the appliance where the active instance is located.
2. Navigate to the **Application instances** section of the **System topology** page and locate the instance that you want to change the replication role of. If it is running, click **Actions** > **Stop**.
3. Click **Actions** > **Change replication role**.

   Alternatively, you can navigate to the **Remote replication** page, locate the instance, and click **Change replication role**.

   You are redirected to the Activity Monitor to view the progress.
4. If you use DNS, and the server is different on the other appliance, update your media servers and clients with the new settings.
5. Ask the other appliance administrator to start the instance.

Unlinking active and replica instances

In the event of a disaster scenario or after a migration, you can unlink the active and the replica instances. The replica instance becomes a separate, standalone instance. Once the instances have been unlinked, you cannot link them again, and you must choose one to use as your primary server going forward.

Use the following procedure to unlink an active and a replica instance.

To unlink an active and a replica instance

1. Sign in to the Flex Appliance Console on either appliance.
2. Navigate to the **Remote replication** page. Locate the instance that you want to unlink. Under **Replication status**, click **Unlink from replica** or **Unlink from active instance**.

   Alternatively, you can navigate to the **Application instances** section of the **System topology** page. Click **Actions** > **Unlink from replica** or **Unlink from active instance**.

   Note: If you unlink from the active instance, the instance must be stopped.

   You are redirected to the Activity Monitor to view the progress.
3. When possible, the replication settings are removed from both appliances as part of the unlink operation. However, in some cases, the settings may remain on the paired appliance. If the settings remain, perform the unlink operation again from that appliance.
4. If you use DNS and want to use the instance that was previously the replica, update your media servers and clients as needed with its settings.
5. Start the instance that you want to use. Do not start both of the unlinked instances.
6. If both appliances are still accessible, delete the instance that you are not using. See “Deleting an application instance” on page 98.

   Note: Depending on the application version and the lockdown mode of the appliance, the instance may need to be running before you can delete it. If you used the same IP address for the active and the replica instance, you must first change the IP address to a different, temporary address before you can start the instance that you want to delete. See “Editing instance network settings” on page 87.

Once you have unlinked the instances, Cohesity strongly recommends that you create a new replica as soon as possible.

Forgetting a paired appliance

Use the following procedure to forget a paired appliance. All pairing information is removed from both of the appliances.

To forget a paired appliance

1. Sign in to the Flex Appliance Console on either appliance. If you haven't already, unlink all active and replica instances.

   See "Unlinking active and replica instances" on page 121.

2. Navigate to the **Remote replication** page. In the **Paired appliances** section, click **Forget this appliance**.
3. In the confirmation window that appears, click **Forget this appliance**. You are redirected to the Activity Monitor to view the progress.
4. When the operation completes, the appliance that you started the operation from attempts to notify the other appliance of the change. In some scenarios, the notification may not be possible. If the paired appliance information remains on the **Remote replication** page of the other appliance, repeat these steps on the other appliance.

Chapter 8

Appliance security

This chapter includes the following topics:

Security overview

Flex Appliance includes multiple features to ensure the security of your data. Each element of the appliance is tested for vulnerabilities using both industry standards and advanced security products. These measures ensure that exposure to unauthorized access and resulting data loss or theft is minimized.

Flex Appliance also uses the Security Technical Implementation Guide (STIG) template to meet security requirements per the Defense Information Systems Agency (DISA) profile.

The security features in this release include but are not limited to the following:

- OS security hardening, including Security-Enhanced Linux (SELinux).
- Forced password changes during initial configuration to make sure that the default password does not remain active on the system.
- The ability to set your own password policy, including the option to use STIG for validation.
  See “Changing the password policy” on page 62.

- No root access from the Flex Appliance Console.
- Lockdown mode and WORM storage support, which let you set additional access restrictions and block data deletion during a specified retention period.
  Lockdown mode also restricts root access from the Flex Appliance Shell.
- The ability to add a sign-in banner that appears before a user signs in to the Flex Appliance Console and the Flex Appliance Shell.
  See "Using a sign-in banner" on page 129.
- Support for external certificates.
  See "Using an external certificate" on page 130.
- Support for multifactor authentication, including the ability to enforce it for all Flex Appliance Console users.
  See "Managing multifactor authentication" on page 64.
- Session timeouts that automatically sign users out of the Flex Appliance Console and the Flex Appliance Shell after 10 minutes of inactivity.
- Conformance to the Federal Information Processing Standards (FIPS) 140-2.
- Password protection in the Flex Appliance Console that locks local user accounts after three sign-in attempts with incorrect passwords. If a security administrator account becomes locked, it is unlocked automatically after 30 minutes. If a different local user account becomes locked, that user and a security administrator must work together to unlock it.
- Sign-in protection in the Flex Appliance Console that locks user accounts with multifactor authentication for 15 minutes after three sign-in attempts with incorrect codes.
- Login protection in the Flex Appliance Shell that locks the **hostadmin** account for 15 minutes after three login attempts with incorrect passwords or multifactor authentication codes.
- Password protection that restricts access to the **GRUB** menu except with assistance from Technical Support. If you need to edit GRUB, contact Technical Support and ask your representative to reference article 100048098.
- Support for Transport Layer Security (TLS) anonymous authentication versions 1.3 and 1.2 for all connections to the appliance except for SNMP connections. Version 1.3 is used by default, while version 1.2 is available for backwards compatibility.
  SNMP connections use the User-based Security Model (USM).
- Mandatory access controls that limit resource access only to those programs and activities that require it, regardless of their system privileges.

- A built-in firewall that blocks all access except for the ports that are required for backup and management.
- Namespaces that partition system resources into distinct, isolated compartments. Each instance gets its own "view" of these resources, which prevents processes within one instance from seeing or interfering with processes or resources in another instance or on the appliance.
  Instances are also assigned limited-service privileges that define which executables and system calls are allowed without the need for elevated system privileges. Moreover, NetBackup services are separated from the backup images that are stored on WORM instances.

Also note the following information regarding the appliance security:

- IP forwarding is enabled in Flex Appliance by design; it is used to facilitate network communication between application instances and external networks.
- Simultaneous multithreading (smt) is enabled by default on the 53xx appliance. The following vulnerabilities affect this feature:
  - CVE-2018-12130
  - CVE-2018-12126
  - CVE-2018-12127
  - CVE-2019-11091

  You can disable smt to address these vulnerabilities; however, significant performance degradation may occur. If you want to disable smt, contact Technical Support and ask your representative to reference article 100046154.

About lockdown mode

Flex Appliance lockdown mode offers additional security levels to protect your appliance and data, in addition to the hardened, secure operating environment that comes out of the box.

Lockdown mode provides the following benefits:

- It prevents unauthorized access or modification to the underlying operating system (OS). Once lockdown mode is enabled, administrators cannot make changes to the OS or the internal components.
  If you need access to the OS for emergency operations, an access key is required to temporarily unlock the appliance. This functionality prevents unauthorized changes even if a malicious actor gained access to stolen credentials.

- It includes the option to create WORM storage instances that prevent your data from being encrypted, modified, or deleted. WORM is the acronym for Write Once Read Many. Any data that is saved on these instances is protected with the following security measures:
  - Immutability
    This protection ensures that the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
  - Indelibility
    This property protects the backup image from being deleted before it expires. The data is protected from malicious deletion.
  - Compliance clock
    The fundamental attribute of WORM is the ability to accurately measure elapsed time to ensure the duration of data retention. The compliance clock is independent of the operating system time and the Network Time Protocol (NTP). It cannot be edited.

Administrators can manage lockdown mode through the Flex Appliance Console. Only administrators with security administrator role can enforce lockdown mode.

Lockdown mode can be enabled at the appliance level using the Flex Appliance Console.

Warning: Lockdown mode does not block access to the remote management (IPMI) port. Cohesity recommends that you set up your network to restrict access and only allow security administrators or the users that manage the physical hardware to use the port.

Lockdown mode must be enabled in the appliance before you can create WORM storage instances.

For more information on creating and managing WORM storage instances, see the *NetBackup Application Guide for Flex Appliance*.

Lockdown mode behavior

- You can enable or disable at the appliance level. When disabled, the appliance does not receive any of the security benefits associated with lockdown mode. Disabled mode is the default appliance state and does not support WORM storage.
  When lockdown mode is enabled, the default mode is enterprise mode.
- After a new installation of Flex Appliance, the **Lockdown mode** dialog will appear at every login until the administrator explicitly enforces or opts out. If the

dialog is closed without making a choice, the user remains on the home page, and the **Lockdown mode** screen will reappear on subsequent logins. An opt-out without providing a reason is treated as no choice, so the dialog continues to appear at each login.

- There is no change to the appliance lockdown mode during platform upgrade.
- During upgrade, instance specific lockdown mode configuration files are created for immutable storage instances if the appliance was in enterprise or compliance mode. The instance lockdown mode remains the same as appliance lockdown mode prior to upgrade. If the lockdown mode was disabled, no instance specific lockdown mode configuration files are created.
- If appliance lockdown mode was disabled before upgrade, you are prompted to enforce the lockdown mode on each login until a selection is made.
- If lockdown mode is enabled, you can disable the lockdown mode only if you have not configured immutable instances. If immutable instances are configured, then you need to delete them before you can disable the lockdown mode.

Managing lockdown mode at the appliance level

You can manage the appliance lockdown mode from the Flex Appliance Console. You can either enable lockdown mode or disable lockdown mode by opting out of it.

If lockdown mode is enabled on appliance, storage reset is disabled. To reset the storage, the appliance lockdown mode must be disabled after deleting all the WORM instances.

Cohesity strongly recommends that you enable lockdown mode to prevent unauthorized access to the OS, even if you do not plan to create WORM storage instances.

Note: If you have a multi-node appliance, make sure that all nodes are configured before you enable lockdown mode.

To enforce the lockdown mode

1. Sign in to the Flex Appliance Console as a security administrator and click **Settings** (gear icon) in the upper-right corner of the page. Under **Security and compliance**, click **Lockdown mode**.
2. On the **Edit** page, select **Enable** and click **Save**.
3. The **Enable lockdown mode** popup appears. Click **Enable lockdown mode**.

   The lockdown mode is updated.

To opt-out of lockdown mode

1. Sign in to the Flex Appliance Console as a security administrator and click **Settings** (gear icon) in the upper-right corner of the page. Under **Security and compliance**, click **Lockdown mode**.
2. On the **Edit** page, select **Disable** and click **Save**.
3. The **Opt out of lockdown mode** popup appears. The popup will walk you through the liability agreement. Read and accept the liability agreement. Click **Next**.
4. Select the reason for opting out of lockdown mode. You can choose any of the listed options or choose **Custom** and specify the reason for opting out.
5. Click **Opt out**.

Managing lockdown mode at the instance level

You can use the Flex Appliance Console to change the lockdown mode on a Flex appliance at the instance level.

Flex Appliance includes the following lockdown modes at the instance level:

- Enterprise mode
  This mode adds additional access restrictions but retains a level of flexibility. In this mode:
  - You can create WORM storage instances.
  - If needed, the application administrator can disable the retention lock on backup images so that they can be expired before the specified retention date.
  - If the instance is on WORM storage server version 19.0.1 or later, security administrators can delete the instances only if no data is present. The application administrator must approve the deletion beforehand.
  - If the instance is on WORM storage server version 19.0 or earlier, security administrators can delete the instance if data is present. The application administrator does not need to approve the deletion beforehand.
- Compliance mode
  This mode adds the highest level of access restrictions. In this mode:
  - You can create WORM storage instances.
  - The retention lock on backup images cannot be disabled before the specified retention date.

- You can delete the instances only if no data is present. If the instance is on WORM storage server version 19.0 or later, the application administrator must approve the deletion beforehand.

Note the following restrictions:

- Only a security administrator can change the lockdown mode.
- You can only change from enterprise mode to compliance mode. Before you change the mode, you must first delete all WORM storage instances.

To change the lockdown mode

1. From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.
2. Locate the row of the application instance for which you want to change the lockdown mode. Click **Action > Change to compliance mode**.
3. In the **Change to compliance mode** popup window, enter the instance name and enter the Flex Appliance Console password. Click **Change mode**.

   The instance mode gets updated and the details are displayed in the **Application instances** section.

Using a sign-in banner

You can set a text banner that appears before a user signs in to the Flex Appliance Console and the Flex Appliance Shell. Typical uses for the login banner include legal notices, warning messages, and company policy information.

To add or edit a sign-in banner

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Sign-in banner**.
2. Click **Add** or **Edit**.
3. Enter the sign-in banner details. You can click **Preview** to see how it appears in the console. When you are finished, click **Save**.

To remove a sign-in banner

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Sign-in banner**.
2. Click **Remove**.

Using an external certificate

By default, the appliance uses a Flex Appliance self-signed certificate for host communication. You can configure the appliance to use an external certificate instead.

Importing an external certificate

To use an external certificate, you must have the following:

- Host certificate: An X.509 certificate for the appliance, in PEM format. This certificate is different from the certificate for your NetBackup primary and media servers.
- Private key: The PKCS #8 private key of the host certificate.
- Passphrase: The passphrase of the private key if the key is encrypted.

To prevent errors while importing certificates, ensure that the external certificate files meet the following requirements.

- All certificate files must have a suffix of .pem or .cer and include `-----BEGIN CERTIFICATE-----` at the beginning of the certificate.
- All certificate files must contain the Flex Appliance Console FQDN in the common name or the subject alternative name (SAN) field of the certificate.
- The subject name and common name fields must not be left empty.
- Only ASCII 7 characters can be used in the subject and SAN fields of the certificate.
- The private key must be in the PKCS #8 PEM format, and it must begin with a header line of `-----BEGIN ENCRYPTED PRIVATE KEY-----`, `-----BEGIN PRIVATE KEY-----`, or `-----BEGIN RSA PRIVATE KEY-----`.
- Flex Appliance's web service uses the PKCS #12 standard and requires certificate files to be in the X.509 (.pem) format. If you obtained the certificate and private key in any other format you must first convert them to the X.509 (.pem) format.

To import an external certificate

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **External certificate**.
2. Upload the required files and click **Next**.
3. Confirm the details and click **Import**.

Removing an external certificate

Use the following procedure to remove an external certificate that you imported. Note that if you remove an external certificate, the appliance reverts to use the default Flex Appliance self-signed certificate for host communication.

To remove an external certificate

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **External certificate**.
2. Click **Remove**.

Using network access control

You can use the network access control feature to control which IP addresses are allowed to access the appliance. Use HTTPS access control to control which IP addresses can access the Flex Appliance Console or the APIs through HTTPS. Use SSH access control to control which IP addresses can access the Flex Appliance Shell through SSH.

To configure or edit network access control

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Depending on which service you want to configure, click **Configure** or **Edit** under **HTTPS access control** or **SSH access control**.
3. Follow the prompts to add the IP addresses or subnets that you want to have access to the appliance. Any IP addresses that are not included in the allowed list cannot access the appliance.

   Note the following information:

   - The IP protocol of the addresses in the allowed list must match the protocol of the appliance.
   - Subnets must be entered in CIDR notation. For example, 1.1.1.0/24.
   - If you use the Dynamic Host Configuration Protocol (DHCP), add subnets instead of IP addresses.
   - For HTTPS access control, you must include your current IP address in the allowed list. It can be entered by itself or as part of a subnet.
   - For SSH access control, you can leave the allowed list empty to block all SSH access.

To disable or enable network access control

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Depending on which service you want to disable or enable, click **Edit** under **HTTPS access control** or **SSH access control**.
3. Deselect or select the check box next to **Enable HTTPS access control** or **Enable SSH access control**.

Changing the SSH port

By default, SSH access to the Flex Appliance Shell uses port 22. If you need to use a different port, use the following procedure to change it.

To change the SSH port

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Network Access Control**.
2. Under **SSH access control**, click **Configure** or **Edit**.
3. Enter a new port in the **SSH port** field and click **Save**.

Recommended settings for the remote management (IPMI) port

This section lists the recommended settings for the remote management (IPMI) port that is used to connect to the Veritas Remote Management Interface.

Cohesity recommends that you adhere to the following guidelines:

- Do not create accounts with null usernames or passwords.
- Add more than one administrative user so that you do not lose access if a password is lost.
- Disable any anonymous users.
- To mitigate the CVE-2013-4786 vulnerability:
  - Use Access Control Lists (ACLs) or isolated networks to limit access to the remote management interface.
  - Keep the IPMI protocol port (623) turned off when not in use to mitigate security risks associated with the IPMI protocol. For more information, see https://nvd.nist.gov/vuln/detail/CVE-2013-4786.

Chapter 9

Monitoring the appliance

This chapter includes the following topics:

Registering an appliance

Registering your appliance is a vital step in allowing Cohesity the ability to help maximize availability of your appliance and provide proactive monitoring support. Registration provides accurate contact details and site-specific information, which aids in expediting support, field services, and customer notification of failures.

To register your appliance, sign in to the System Health Insights portal (https://systemhealth.netinsights.cohesity.com) with your MyCohesity credentials.

For more information, see the *Appliance AutoSupport Reference Guide* and the *System Health Insights User Guide*.

Configuring alerts

The appliance has the ability to monitor itself and send a notification if it detects a problem that needs attention. You can configure the following types of alerts from the Flex Appliance Console:

- Call Home
  Send notifications to Cohesity and the NetInsights Console. Call Home is enabled by default.
  See "About AutoSupport and Call Home" on page 134.
  See "Configuring Call Home" on page 134.
- Email alerts
  Send notifications to an email address.
  See "Configuring email alerts" on page 135.
- SNMP alerts
  Send notifications to an SNMP manager.
  See "Configuring SNMP alerts" on page 136.

About AutoSupport and Call Home

AutoSupport is a set of infrastructures, processes, and systems that enhance the support experience through proactive monitoring of appliance hardware and software. AutoSupport also provides automated error reporting and support case creation.

Call Home provides information regarding appliance component states and status. AutoSupport correlates the Call Home data with other site configuration data that is held for technical support and error analysis. With AutoSupport, the customer support experience is greatly improved.

More information about AutoSupport and Call Home is available in the *Appliance AutoSupport Reference Guide* at the following site:

Appliance documentation

Configuring Call Home

The appliance can communicate with the Call Home server and upload hardware and software information. If required for your environment, you can also configure a proxy server.

Use the following procedures to manage the Call Home configuration.

To configure or edit Call Home

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Call Home**.
2. Click **Configure** or **Edit**.
3. If required, select **Enable proxy server** and fill in the required details. Then click **Configure** or **Save**.

   Note: If your appliance is configured with an IPv6 address and your proxy server is configured with both IPv4 and IPv6 addresses, you must do one of the following for alerts to work:

   Enter the server IPv6 address instead of the hostname.

   After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 157.

   If you use DNS, modify your DNS configuration so that the server hostname only responds to the IPv6 address.

4. To test the connection, wait at least 10 seconds and then click **Test Call Home**.

To disable or enable Call Home

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Call Home**.
2. Click **Disable** or **Enable**.

Configuring email alerts

You can configure the appliance to send emails with alerts about the hardware, the appliance services, and your application instances.

Note: NetBackup alerts must be configured separately from NetBackup. See the topic "Setting up mailx email client" in the *NetBackup Administrator's Guide, Volume I*.

Use the following procedures to manage email alerts.

To configure or edit email alerts

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Email alerts**.
2. Click **Configure** or **Edit**.

3 Fill in the required details and click **Configure** or **Save**.

Note: If your appliance is configured with an IPv6 address and your SMTP server is configured with both IPv4 and IPv6 addresses, you must do one of the following for alerts to work:

Enter the server IPv6 address instead of the hostname.

After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 157.

If you use DNS, modify your DNS configuration so that the server hostname only responds to the IPv6 address.

---

4 To test the connection, wait at least 10 seconds and then click **Test**.

To disable or enable email alerts

1 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Email alerts**.

2 Click **Disable** or **Enable**.

Configuring SNMP alerts

The Simple Network Management Protocol (SNMP) enables you to monitor the appliance performance. You must have an existing SNMP manager before you can configure SNMP alerts.

Use the following procedures to manage SNMP alerts.

To configure or edit SNMP alerts

1 Locate the Flex Appliance MIB file at the following website:
https://sort.veritas.com/netbackup/utility_tool

Copy the contents of this file to your SNMP manager to set it up to receive appliance monitoring traps.

Note: If you use SNMPv3, the appliance engine ID may be required by your SNMP manager. See the following article for the steps to calculate the engine ID: How to calculate the appliance engine ID for SNMPv3

---

2 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **SNMP alerts**.

3 Click **Configure** or **Edit**.

4 Fill in the required details and click **Configure** or **Save**.

Note: If your appliance is configured with an IPv6 address and your SNMP server is configured with both IPv4 and IPv6 addresses, you must do one of the following for alerts to work:

Enter the server IPv6 address instead of the hostname.

After alert configuration, add the server IPv6 address to the appliance Hosts file. See "Changing DNS or Hosts file settings" on page 157.

If you use DNS, modify your DNS configuration so that the server hostname only responds to the IPv6 address.

---

5 Wait at least 10 seconds and then click **Test** to send a test SNMP trap.

To disable or enable SNMP alerts

1 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **SNMP alerts**.

2 Click **Disable** or **Enable**.

Setting the threshold values for disk usage alerts

You can set the threshold at which alerts are sent for high disk usage. The default value is 80%.

Note: Critical `diskspace` alerts are sent when disk usage exceeds 90%. This threshold cannot be changed. In some cases, backup jobs may be affected before you reach the 90% threshold, so Cohesity recommends that you add storage or otherwise address the issue as soon as you see an alert.

To set the threshold value

1 Log in to the Flex Appliance Shell.

2 Run the following command:

```
set alerts diskspace-threshold threshold=<value>
```

Where <*value*> is an integer between 0 and 89. If you enter 0, disk usage alerts are disabled. Cohesity recommends that you do not set this value higher than 85.

3 If you have a multi-node appliance, repeat these steps on the other node.

To view the threshold value

1. Log in to the Flex Appliance Shell.
2. Run the following command:

```
show alerts diskspace-threshold
```

Viewing performance metrics

Depending on the information that you want to see, you can view performance metrics from the Flex Appliance Console or the Flex Appliance Shell.

Viewing performance metrics from the Flex Appliance Console

You can view performance metrics of the nodes and the application instances from the **Home** page on the Flex Appliance Console. Locate the **Performance** section and use the tabs to switch between the nodes and the instances.

Note the following information about how the node and the instance data relate to each other:

- The percent of CPU that all instances use should add up to approximately the same percent of CPU that the nodes use. If it does not, there may be an issue with the appliance.
- The **Available memory** graph for the nodes shows how much memory is available, whereas the **Memory utilization** graph for the instances shows how much memory is used.
- The **Network throughput** graph for the nodes shows how much data is transferred and received per network interface. If an interface is shared with multiple instances, it shows the cumulative throughput across those instances. The **Network throughput** graph for the instances shows how much data is transferred and received per interface on that instance only.

Viewing performance metrics from the Flex Appliance Shell

You can view live performance metrics of all of the instances on your appliance from the `support shell` command view in the Flex Appliance Shell.

To view instance performance metrics from the Flex Appliance Shell

1. Log in to the Flex Appliance Shell on the node that you want to view performance metrics for.
2. To view metrics for all instances, enter the following commands:

- `support shell`
- `podman stats --no-stream`

To view metrics for a specific instance, enter the following commands:

- `support shell`
- `podman stats --no-stream <instance name>`

The following information displays for each of the instances on the node, including the Flex Appliance infrastructure instances:

- `CID`: An instance identifier
- `CPU`: The CPU usage of the instance
- `MEM`: The memory usage of the instance
- `NET RX/TX`: The amount of data that is being transmitted and received
- `IO R/W`: The amount of data that is being read from and written to the instance storage disk(s)
- `PIDS`: The total number of processes that are running on the instance

3 When you are done reviewing the information, enter **q** to return to the main Flex Appliance Shell view.

Monitoring the appliance from the System Health Insights portal

System Health Insights is a global appliance monitoring and insights portal that delivers telemetry-driven information to help you understand the health and operational state of your appliances.

You can use System Health Insights to monitor storage use across appliances, inode usage, monitor the hardware metrics, and reduce update planning with automatic updates.

For more information about System Health Insights, see the *System Health Insights User Guide*.

Inode usage monitoring and alerting

Some filesystems or volumes in Flex Appliance are provisioned with a fixed number of inodes at creation time. Unlike disk capacity, inode count cannot grow dynamically. A filesystem with exhausted inodes causes critical failures across the instance.

When inode consumption reaches 100%:

- No new files or directories can be created on the volume, even if sufficient free disk space remains.
- Application and platform services may fail to write logs, metadata, or state files.
- Critical NetBackup operations may be interrupted.
- Instance level services may malfunction, leading to degraded functionality or downtime.

To prevent service disruption caused by inode exhaustion, Flex Appliance introduces inode usage monitoring and alerting for all application instance volumes.

Key features:

- Collection of inode usage for every application instance volume
- Metrics flow into the central telemetry system for visualization.
- Administrators can use these insights to take preemptive action before inode exhaustion affects service availability.
- Exposure of inode metrics for platform wide monitoring and troubleshooting
- Automated alerting when inode usage reaches predefined thresholds.
  - Email and SNMP alerts are automatically sent to configured recipients.
  - SHI alerts appear in the UI under **System > Events** tab.

Benefits

- Early detection of inode pressure on Flex volumes.
- Prevention of service interruptions caused by inability to write logs or metadata.
- Improved troubleshooting with accurate inode consumption metrics.
- Better operational reliability for applications running on Flex.

Flex Appliance captures and exposes the following per volume inode metrics:

Metric Name	Description
storage_filesystem_files	Total number of inodes available on the filesystem
storage_filesystem_files_used	Number of inodes currently consumed

These metrics are made available to the platform's monitoring and observability pipeline for dashboards, analysis, and automated alert evaluation.

Inode utilization is continuously monitored. Flex Appliance triggers alerts based on the following thresholds:

- Warning Threshold (80%)
  - Triggered when inode usage reaches 80% of available inodes.
  - Generates:
    - Warning level email alert
    - SHI (System Health Indicator) warning alert
- Critical Threshold (90%)
  - Triggered when inode usage reaches 90% of available inodes.
  - Generates:
    - Critical level email alert
    - SHI critical alert

Both alert types include details such as:

- Affected instance and volume
- Total inodes
- Used inodes
- Current utilization percentage
- Recommended corrective actions such as cleaning unnecessary files, increasing filesystem size, or reprovisioning

Viewing the hardware status

You can use the `show` command view in the Flex Appliance Shell to obtain information about the appliance hardware components. The hardware monitoring commands are available before initial configuration.

See "Viewing node information" on page 141.

See "Viewing storage shelf information on a 52xx appliance" on page 144.

Viewing node information

Depending on the appliance model, you can view data about the following compute node components from the shell. Details are provided as needed.

- All (components)
- Adapter
- CMOSBattery

- Connection (between the appliance and the Primary Storage Shelf)
- CPU
- DIMM
- DIMMPopulation
- Disk
- Fan
- FibreChannel
- Firmware
- Network
- PCI
- Power
- Product
- RAID
- ReservedStorage
- SED
- SSD
- StorageConnections
- StorageStatus
- Temperature
- VROC

To view node component health

1. Log in to the Flex Appliance Shell, and type the following.

   `show hardware-health node component=<component>`

2. Press **Enter** to view the data.

Viewing storage shelf information on a 53xx appliance

You can view data about the storage shelf components from the shell with the `show hardware-health primaryshelf` command, the `show hardware-health expansionshelf` command, and the `show hardware-data storage-shelf` command.

The `show hardware-health primaryshelf` command shows details about the following components for a primary shelf:

- All (components)
- BBU (battery backup unit)
- Controller
- Disk
- Fan
- Firmware
- Power
- Product
- Temperature
- Volume
- VolumeGroup

The `show hardware-health expansionshelf` command shows details about the following components for a specific expansion shelf:

- All (components)
- Disk
- Fan
- Firmware
- Power
- Product
- Temperature
- Volume
- VolumeGroup

The `show hardware-data storage-shelf` command shows more granular details about the following components for all storage shelves:

- configuration
- controllers
- disk-affinity
- disk-group-statistics
- disk-groups

- disk-statistics
- disks
- enclosures
- events
- pools
- ports
- sensor-status
- system
- volumes

To view storage shelf component status

1. Log in to the Flex Appliance Shell.
2. Run one of the following commands:
   - For a primary shelf:
     `show hardware-health primaryshelf component=<component>`
     Where <*component*> is the component that you want to see information for.
   - For an expansion shelf:
     `show hardware-health expansionshelf component=<component> shelf_id=<shelf number>`
     Where <*component*> is the component that you want to see information for and <*shelf number*> is the number of the expansion shelf, starting from 1.
   - For more granular details about all storage shelves:
     `show hardware-data storage-shelf <component>`
     Where <*component*> is the component that you want to see information for.

Viewing storage shelf information on a 52xx appliance

You can view data about the following storage shelf components from the shell:

- All (components)
- Disk
- Fan
- Power

- Product
- Temperature

To view the storage shelf status

1. Log in to the Flex Appliance Shell.
2. Run the following command:

   ```
   show hardware-health storageshelf component=<component>
   ```

   Where *<component>* is the component that you want to see information for.

Viewing hardware faults

From the Flex Appliance Shell you can run a command that shows only hardware component faults.

To view hardware faults

1. Log in to the Flex Appliance Shell, and type the following.

   ```
   show hardware-errors
   ```

2. Press **Enter** to display the data.

Viewing system data

In addition to individual hardware component data you can obtain information about the appliance system. The `self-test` command captures more data than the `hardware-health` command. It includes a health check all the way to the NetBackup application layer.

This section provides the information that is specific to the output from the `self-test` commands. The available information is provided in the following table.

Table 9-1 Self-test data

Command	Description
`disk`	Shows the current status of the storage array.
`software`	Shows the current status of the various appliance software components.
`hardware`	Shows the current status of the various appliance hardware components.

Table 9-1 Self-test data *(continued)*

Command	Description
`network`	Shows the current status of the network connections.

To view appliance system data

1 Log in to the Flex Appliance Shell, and type any of the following as needed.

```
system self-test disk
system self-test software
system self-test hardware
system self-test network
```

2 Press Enter after each string to view the data.

See "Gathering logs" on page 175.

Clearing the hardware status

If you replace a hardware component or experience any issues with the hardware monitoring data, you may need to clear the hardware status. When you clear the status, all component statuses are reset. When you recheck the monitoring data, the most current information shows.

To clear the hardware status

1 Log in to the Flex Appliance Shell.

2 Run the following command:

```
support clear-hardware-status
```

3 Follow the prompts to confirm.

Note: After the status is cleared, the collection of new data takes approximately 15 minutes. During that time, the hardware monitoring commands do not show any data.

Forwarding logs

You can forward the appliance system logs (syslogs) and the audit logs to an external log management server. Your log management server must support the Rsyslog client.

Flex Appliance supports the following:

- TLS Anonymous Authentication for log forwarding
- X.509 file format for certificate files

To configure or edit log forwarding:

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Log forwarding**.
2. Click **Configure** or **Edit**.
3. Enter the log forwarding settings. If you want to secure the log transmissions from the appliance to the log server, select **Enable TLS log transmission** and upload the required certificate files. Cohesity recommends that you enable TLS for security purposes.
4. When you are finished, click **Save**.

To stop forwarding logs

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Log forwarding**.
2. Click **Remove**.

Providing access for external monitoring

You can generate a predefined API token to provide access to the appliance for external monitoring or support.

The following token types are available:

- Metrics token: Monitor the performance metrics from a third-party analytics application. For example, Grafana.
- Support token: Grant permission to Technical Support to create, download, and clean up log packages on the appliance.

Only one token of each type is allowed at a time.

To generate a predefined API token

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Predefined API tokens**.
2. Click **Generate**.
3. Select the token type and enter the required details. When you are finished, click **Generate**.
4. A pop-up window appears with the token.

   Note: Make sure that you copy the token and save it to a safe location. You can no longer view it after you close the window.

5. Use the new token to provide access to your analytics application or share it with Technical Support. You can access the `metrics` APIs with the metrics token and the `logscollect` APIs with the support token. Check SORT for more information on the APIs.

Revoking access for external monitoring

Use the following procedure to delete a predefined API token and remove access privileges for an external monitoring service or Technical Support.

To delete a predefined API token

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Predefined API tokens**.
2. Select the token that you want to delete and click **Delete**.

Chapter 10

Managing self-encrypting drives (SEDs) on a Flex 53x2 appliance

This chapter includes the following topics:

About self-encrypting drives (SED) on Flex 53x2 appliances

Flex Appliances support models with built-in self-encrypting drive (SED) capabilities to help protect data at rest. The 53x2 Flex Appliance series includes operating system and storage drives that support self-encryption and are referred to as SED models.

On SED-enabled systems, encryption is handled at the drive level to ensure that data remains protected even if a drive is removed from the appliance. When the operating system drives are secured using the default platform key, the system automatically attempts to unlock the drives during the boot sequence, requiring no user intervention.

Changing an SED key

Appliances with self-encrypting drive (SED) capability use encryption keys to protect the drives. Each node in a multi-node appliance has its own key. The storage shelves share another key. You can see the last time that the key was changed from the **System topology** page.

Use the following procedure to change the SED encryption key on an appliance node or the storage shelves.

Note: This procedure requires a user with the SED key administrator role. If you have not assigned the SED key administrator role yet, see the topic "Managing Flex Appliance Console users and tenants" in the *Flex Appliance Getting Started and Administration Guide*.

To change an SED key

1. Sign in to the Flex Appliance Console as an SED key administrator and navigate to the **System topology** page.
2. Locate the widget for the nodes or the storage and click **Rekey** next to the device that you want to change the key for.
3. Follow the prompts to change the key. You can optionally switch from the internal key management service (KMS) to an external KMS if you have added one, or back to the internal KMS.

   See “Adding an external key management service (KMS)” on page 151.

   If you have never changed the key before, use the following default keys for the current key:

   - For a node: The node serial number
   - For the storage: **Encrypt!0nK3y**

4 Click **Rekey**.

5 Follow the prompts in the confirmation window that appears and click **Rekey** or **Switch and rekey**.

Warning: If you use the internal KMS and forget the encryption key, all data becomes lost and unrecoverable. Make sure that you save the new key in a safe location.

Adding an external key management service (KMS)

If your appliance has self-encrypting drives (SEDs), it uses an internal key management service (KMS) by default to manage the encryption keys. If you prefer, you can add an external KMS and use it instead. An external KMS provides enhanced control and security because you manage it outside of the appliance.

Flex Appliance supports the KMIP 1.4 protocol for communication with the external KMS.

Note: To add an external KMS, the storage shelf firmware must be on version I200R005-08 or later. You can check the version with the `show hardware-health primaryshelf component=firmware` command.

Use the following procedure to add an external KMS.

To add an external KMS

1 Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Key management service**.

2 Click **Add KMS**.

Fill in the required information and click **Add**.

3 Once the KMS has been added successfully, click **Actions** > **Test KMS connection** to verify the connection.

You can now switch to use the new KMS to manage the encryption keys.

See “Changing an SED key” on page 150.

Editing an external key management service (KMS)

Use the following procedure to edit an external KMS that you added to the appliance.

To edit an external KMS

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Key management service**.
2. Depending on which part of the KMS you need to edit, click **Actions** > **Edit servers**, **Edit port**, or **Edit certificates**.
3. Make the required changes and click **Save**.

Removing an external key management service (KMS)

Use the following procedure to remove an external KMS that you added to the appliance. The KMS cannot be in use.

To remove an external KMS

1. Sign in to the Flex Appliance Console as a security administrator and click the gear icon in the upper-right corner of the page, then click **Key management service**.
2. Click **Actions** > **Remove KMS**.

Unlocking the operating system drive

There are two supported mechanisms for securing and unlocking operating system drives:

- User-managed key
- EKMS-managed key

During a system reboot:

- If the key required to unlock the OS drives is not automatically available, the system prompts the user to manually enter the key.
- For EKMS-managed keys, the unlock key must be entered in hex-encoded format.

- In case of transient failures, you may retry the process by performing an IPMI power cycle.

Note: Avoid using power reset. A power reset after an incorrect key entry is counted as a failed unlock attempt. After two failed attempts combined with power resets, the disks become permanently locked, even if the correct key is entered later.

A power cycle (full off → on) is the recommended method for retrying after any incorrect key entry. This prevents the system from counting the failed attempt toward disk lockout.

About the SED states

The appliance hardware monitoring shows the SED state for your self-encrypting drives (SEDs). It may show any of the following states:

- Not SED Capable
  This state means that the drive is a standard drive that does not have the hardware encryption capabilities of an SED.
- Not Secured
  This state means that the drive is an SED, but its security features have not been configured yet. In this state, data on the drive is accessible without a password or specific authentication, so it is not protected from unauthorized access.
- Secured, Unlocked
  This state means that the drive is an SED that has been configured and secured with an encryption key, and it is currently unlocked. When the drive is unlocked, the operating system and authorized users have access to the data.
  This state is the normal operating state for an SED.
- Secured, Locked
  This state means that the drive is an SED that has been configured and secured with an encryption key, and it is currently locked. When the drive is locked, the data is inaccessible until you provide the key, even if the drive is physically removed and connected to another system.
  This state is the ideal state for an SED when it is not actively in use.

Moving an appliance with SEDs

Use the following procedure to move an appliance with self-encrypting drives (SEDs).

To move an appliance with SEDs

1. Make sure that the keys for the nodes and the storage are saved in a safe location.

   Warning: If you do not have the keys saved and forget them during the move, all data becomes lost and unrecoverable.

   If you have never changed the keys, the default keys are as follows:

   - For each node: The node serial number
   - For the storage: **Encrypt!0nK3y**

   Use the `show serial-number` command to retrieve the node serial number from the Flex Appliance Shell.

2. Run the following command to clear the stored keys from the appliance:

   ```
   system sed clear-keys
   ```

3. Shut down the appliance and physically turn off the appliance hardware.

   See the section "Shutting down the appliance" in the *Flex Appliance Getting Started and Administration Guide*.

   See “Shutting down the appliance” on page 158.

4. Move the appliance to its new location and turn it on, following the steps in the *Hardware Installation Guide*. You are prompted to enter the key for each node when it starts up.

   Note: If you do not enter the key within fifteen minutes, the node enters emergency mode. Restart the node to return to the key prompt.

5. Run the following command to unlock the storage:

   ```
   system sed unlock-storage
   ```

   Enter the key for the storage when prompted.

Adding or replacing storage

Note the following important information about the storage shelves and drives for the Cohesity 53x2 Appliances.

Adding storage shelves

The procedure to add storage shelves to the Cohesity 53x2 Appliances is different than the other hardware models. The nodes and the existing storage shelves must be on when you add the new shelves.

See the model-specific *Cohesity Appliance Hardware Installation Guide* for the full procedure.

Replacing an SED

If you need to replace a self-encrypting drive (SED), make sure that you adhere to the following requirements:

- The appliance must be powered on.
- The drive must not be locked.
  To check the status of the drives, run the `show hardware-health primaryshelf component=disk` command in the Flex Appliance Shell. Make sure that the status is either `Unsecured` or `Secured, Unlocked`.

For the instructions on how to replace the drive, refer to the following document:

Replacing a disk drive carrier in a Veritas 5U84 Storage Shelf

Chapter 11

Reconfiguring the appliance

This chapter includes the following topics:

Reconfiguring the appliance network

Use the following procedure to reconfigure the appliance network after initial configuration.

Note: You cannot change the hostnames of the nodes or the Flex Appliance Console.

To reconfigure the network

1. Stop all application instances.
2. Log in to the Flex Appliance Shell from the Veritas Remote Management Interface. If you have a multi-node appliance, you can log in to either node.
3. If DNS is not configured for the current configuration, you must update the hostname resolution information in the appliance `Hosts` file before you reconfigure the network. Update the required information for the node and the Flex Appliance Console.

   See "Changing DNS or Hosts file settings" on page 157.
4. Run the following command:

   ```
   setup configure-network
   ```
5. Follow the prompts to enter the host network information. You can enter up to three DNS server IP addresses with a comma-separated list. If you need to add more, you can use the `set network dns` command after the reconfiguration.

Note: You can use IPv4 or IPv6 addresses for the appliance, but a dual-stack network is not supported. If you change the protocol, the protocol that was originally configured becomes disabled.

Changing DNS or Hosts file settings

Use the following procedures to change the DNS or `Hosts` file settings after initial configuration.

Changing DNS settings

To change the DNS server IP address or search domain

1. From the Flex Appliance Shell, run the following command:

   ```
   set network dns
   ```
2. Follow the prompts to change the DNS settings as follows:
   - To replace the existing settings with new parameters, enter the new information in the appropriate fields. You can enter multiple DNS server IP addresses or search domains using a comma-separated list.
   - To remove the DNS settings, leave the fields blank.

Warning: If you remove existing DNS settings, you must add the hostname resolution information to the appliance `Hosts` file. See the section called "Changing Hosts file settings" on page 158.

Changing Hosts file settings

If you do not want to use DNS or want to bypass DNS for specific hosts, you can use the appliance `Hosts` file to manage the hostname resolution information.

To add entries to the `Hosts` file

1. Gather the following information for all appliance nodes and for the Flex Appliance Console, if applicable:
   - IP address
   - Hostname
   - Domain
2. From the Flex Appliance Shell, run the following command:

   ```
   system add-host
   ```
3. One at a time, enter the required information for the nodes and the Flex Appliance Console, if applicable.

To remove an entry from the `Hosts` file

1. From the Flex Appliance Shell, run the following command:

   ```
   system remove-host
   ```
2. Enter the IP address of the host that you want to remove.

Shutting down the appliance

Use the following procedure to shut down your appliance.

To shut down an appliance

1. Stop all instances from the Flex Appliance Console.
2. Log in to the Flex Appliance Shell.
3. Do one of the following:
   - If you have a 5150 or a 52xx appliance, or if you have a 53xx appliance and do not want to turn off the storage shelves, run the following command:

     ```
     system shutdown
     ```

- If you have a 53xx appliance and want to turn off the storage shelves, Cohesity recommends that you shut them down first.

  Warning: Shutting down the storage shelves is not mandatory, but if you do shut them down, you must also use the power button to turn them off. Only shut down the shelves if you are prepared to do so.

  To shut down the storage shelves, use the following steps:

  - If you have a multi-node appliance, first shut down one of the nodes with the `system shutdown` command. Then log in to the other node.
  - Run the following command:

    ```
    support storage-shelf shutdown
    ```

    This command also shuts down the node that you ran the command from.

4. If you shut down the storage shelves, use the power button to turn off the primary shelf. Wait until the fans have stopped spinning, all noises have stopped, and all lights on the front panel are off. Then do the same for the expansion shelves, in order from the one that is closest to the nodes to the one that is farthest from the nodes.

   If you also need to physically turn off the appliance nodes, unplug the power cables.

   Note: When you turn the appliance and the shelves back on, you must do so in the reverse order that you turned them off. Follow the instructions in the *Hardware Installation Guide* for your appliance.

Performing a factory reset

The purpose of a factory reset is to return a node to a clean, unconfigured, factory state. A factory reset discards all configuration data but does not affect the storage data. If you have a multi-node appliance, a factory reset only affects the node that you run this procedure from.

A factory reset resets the node to the current version. However, if you installed any security patches, they must be reinstalled after the factory reset.

After you perform a factory reset, you can also reset the storage if your appliance is not in lockdown mode. If it is in lockdown mode, storage reset is disabled.

Note: If more than the tested number of Fibre Channel devices or paths are connected to the appliance, Cohesity recommends that you disable the ports or disconnect the devices before you begin this procedure. When the procedure is complete, reenable or reconnect them. You may need to scan the ports from the Fibre Channel interfaces page.

See "Managing the appliance Fibre Channel ports" on page 41.

To perform a factory reset

1. If you have a multi-node appliance, remove the node that you want to reset from the appliance. If you want to reset both nodes, choose a node to begin the procedure with and remove that node. See "Removing a node" on page 171.
2. Log in to the Flex Appliance Shell from the node that you want to reset.

   Note: Cohesity recommends that you log in from the Veritas Remote Management Interface instead of an SSH session to perform a factory reset. To access the Veritas Remote Management Interface, refer to the initial configuration procedure. See "Performing the initial configuration" on page 22.

3. Enter the following command:

   ```
   system factory-reset
   ```

4. Type `yes` to continue, and then press **Enter**.

   Note: Once you have started the `factory-reset` operation, do not perform any other tasks on the appliance until the reset is complete.

   When the process is complete, you are prompted to restart. The factory reset is not complete until after the system is restarted. The system continues to run with the current configuration until after the restart is completed.

5. Do one of the following:
   - To restart the node now, type `yes`, and then press **Enter**.
   - To restart the node later, type `no`, and then press **Enter**.
     You can type the following command at any time to restart:
     ```
     system restart
     ```

6 When the restart is complete, the **hostadmin** user password resets to the default password (**P@ssw0rd**). Use the default password to log back in to the Flex Appliance Shell, then run the following command to change the password:

```
set user password
```

7 If you have a multi-node appliance and want to reset both nodes, repeat the procedure on the other node.

Next steps for a single-node appliance

After the factory reset is complete, do one of the following:

- If you want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 170.
  See "Performing the initial configuration" on page 22.
- If you do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 168.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 22.

Next steps for a multi-node appliance

After the factory reset is complete, do one of the following:

- If you performed the factory reset on only one of the nodes, add it back to the appliance. If the node was previously updated, reinstall the update after you add it back.
  See "Adding a node" on page 25.
- If you performed the factory reset on both nodes and want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 170.
  See "Performing the initial configuration" on page 22.
- If you performed the factory reset on both nodes and do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 168.

Performing a reimage

The purpose of a reimage is to remove and reinstall the appliance software on a node. Cohesity recommends that you always try a factory reset before resorting to a reimage.

A reimage does not affect the storage data. After you perform a reimage, you can also reset the storage if desired.

Warning: This procedure cannot be run on a 5340 appliance. If you need to reimage a 5340 node, you must contact Technical Support. Ask your representative to reference article 100044669.

Use one of the following procedures to reimage an appliance.

Reimaging from the USB drive

To reimage an appliance from the USB drive

1. Before you begin the reimage process, Cohesity recommends that you record the configuration information that you entered when you performed the initial configuration.
2. Create the USB drive. See the following article for instructions: How to create a Flex Appliance USB flash drive
3. Verify that the following ports are connected to the network:
   - The remote management (IPMI) port
     Used to connect to the Veritas Remote Management Interface
   - host0
     Used to connect to the Flex Appliance Console
4. Insert the USB drive into a USB port on the node that you want to reimage.
5. Use the following steps to access the Veritas Remote Management Interface:
   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 139 or later recommended (minimum version 105 or later)
     - Mozilla Firefox version 142 or later recommended (minimum version 140 or later)
   - Enter the IP address that is assigned to the remote management port of the node that you want to reimage.

- Log in to the Veritas Remote Management Interface. If you have not previously logged in, use the following default credentials:
  - **User Name**: **sysadmin**
  - **Password**: **P@ssw0rd**

6 If you logged in with the default password, you must change the password before you can configure or recover the appliance after the reimage. Perform the following steps:

- Navigate to **Configuration** > **Users** and select the **sysadmin** user.
- Click **Modify User**.
- Select the **Change Password** check box and enter a new password.

7 Do one of the following to launch the Flex Appliance Shell:

- Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
- If available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**.

Note: Availability of the HTML5 option depends on the appliance firmware version. You can check the version from the **System** > **System Information** page. The BIOS ID must show version 00.01.0016 or later.

---

8 Return to the Veritas Remote Management interface and select **Server Power Control** on the left side of the **Remote Control** page.

9 On that page, do the following:

- Select the **Reset Server** radial option.
- Click **Perform Action**.

10 Return to the Flex Appliance Shell and wait for the system to turn on. When the splash screen appears, immediately press **F6** to enter the **boot** menu.

Note: You only get a window of a few seconds to perform this task. If you miss the window, the operating system loads, and you cannot access the **boot** menu.

---

11 When the **boot** menu appears, scroll down to the USB drive and press **Enter**.

12 The system begins to start from the USB drive. It then presents you with multiple options.

If you have a 5240 or 5x50 appliance, select **Install Veritas Optimised OS** and press **Enter**.

If you have a 5x60 appliance, perform the following steps:

- Select **Install Veritas Optimised OS (RA Appliances Only!)** and press **e**.
- On the following screen, locate the following line:

```
nst.ks=cdrom:/ks.cfg
inst.xdriver=vesamodprobe.blacklist\t=qla2xxx,lpfc,ocs..fc..scst,ahci,isci,ast
pcie_aspm=off
```

- Replace this line with the following text:

```
inst.stage2=hd:LABEL=VxOS inst.ks=hd:LABEL=VxOS:/ks.cfg
inst.repo=hd:LABEL=VxOS:/
```

- Enter **Ctrl +X**.

13 When the installation of the new appliance package is complete, you receive a **Welcome** message in the Flex Appliance Shell. The **hostadmin** user password resets to the default password (**P@ssw0rd**), so use the default password to log back in to the Flex Appliance Shell. Then run the following command to change the password:

```
set user password
```

14 Restart the node with the `system restart` command.

15 Proceed to the next steps that are listed at the end of this topic.

Reimaging from an ISO file

To reimage an appliance from an ISO file

1 Before you begin the reimage process, Cohesity recommends that you record the configuration information that you entered when you performed the initial configuration.

2 Verify that the following ports are connected to the network:

- The remote management (IPMI) port
  Used to connect to the Veritas Remote Management Interface
- host0
  Used to connect to the Flex Appliance Console

3 From a computer within your appliance domain, download the appropriate ISO file from the Download Center on the Support website.

4. Save the ISO file to a local drive of the computer.
5. If a firewall exists between the appliance and the remote devices that manage the appliance, make sure that the following ports are open:
   - 627 RMM ISO/CD
   - 5902 RMM CLI

   Note: These ports are not required for reimages over HTML5. However, note that the performance of HTML5 is significantly slower, and the availability of the option depends on your appliance firmware version. You can check the version from the **System** > **System Information** page. To reimage over HTML5, the BIOS ID must show version 00.01.0016 or later.
6. Turn off the appliance.
7. Use the following steps to access the Veritas Remote Management Interface:
   - Open a supported web browser on a system that has a network connection to the appliance. Flex Appliance supports the following browsers:
     - Google Chrome version 139 or later recommended (minimum version 105 or later)
     - Mozilla Firefox version 142 or later recommended (minimum version 140 or later). Note that reimaging over HTML5 is not supported on Firefox.
   - Enter the IP address that is assigned to the remote management port of the node that you want to reimage.
   - Log in to the Veritas Remote Management Interface. If you have not previously logged in, use the following default credentials:
     - **User Name**: **sysadmin**
     - **Password**: **P@ssw0rd**
8. If you logged in with the default password, you must change the password before you can configure or recover the appliance after the reimage. Perform the following steps:
   - Navigate to **Configuration** > **Users** and select the **sysadmin** user.
   - Click **Modify User**.
   - Select the **Change Password** check box and enter a new password.
9. Do one of the following to launch the Flex Appliance Shell:

- (Recommended) Navigate to **Remote Control** > **Console Redirection** and click **Launch Console**.
- If you are using Google Chrome and the option is available, navigate to **Remote Control** > **iKVM over HTML5** and click **Launch Console over HTML5**. Note that the performance of HTML5 is significantly slower.

10 If you clicked **Launch Console**, perform the following steps:

- When the shell launches, click on the **Device** drop-down menu on the console and select **Redirect ISO**.
- From the **Open** pop-up window that appears, choose the ISO file that you want to install and click **Open**.

11 If you clicked **Launch Console over HTML5**, perform the following steps:

- Navigate to **Virtual Media** > **Virtual Media over HTML5** and click **Launch virtual media over HTML5**.
- In the pop-up window that appears, click **Choose file** and select the ISO file that you want to install, then click **Open**.
- From the **Virtual Media** > **Virtual Media over HTML5** page, click **Mount**.

12 Return to the Veritas Remote Management interface and select **Server Power Control** on the left side of the **Remote Control** page.

13 On that page, since the server is currently off, the only available option is **Power ON Server**.

Click **Perform Action**.

14 Return to the Flex Appliance Shell and wait for the system to turn on. When the splash screen appears, immediately press **F6** to enter the **boot** menu.

Note: You only get a window of a few seconds to perform this task. If you miss the window, the operating system loads, and you cannot access the **boot** menu.

---

15 When the **boot** menu appears, scroll down to **Virtual CDROM** or **UEFI USB Device** and press **Enter**.

16 The system begins to start from the ISO file you selected earlier. It then presents you with the following options:

- **Boot from local drive**
- **Install Veritas Optimised OS**
- **Rescue a Red Hat Enterprise Linux system**

Select **Install Veritas Optimised OS** and press **Enter**.

Note: The remote management ISO installation is sensitive to the quality of the network connection. If an installation failure occurs, try the installation again. If the problem persists, try to improve the quality of the remote management network connection. You can also burn the ISO file onto a DVD and install it with a USB DVD-ROM drive that you physically connect to the appliance.

---

17 When the installation of the new appliance package is complete, you receive a **Welcome** message in the Flex Appliance Shell. The **hostadmin** user password resets to the default password (**P@ssw0rd**), so use the default password to log back in to the Flex Appliance Shell. Then run the following command to change the password:

```
set user password
```

18 Restart the node with the `system restart` command.

19 Proceed to the next steps that are listed at the end of this topic.

Next steps for a single-node appliance

After the reimage is complete, do one of the following:

- If you want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 170.
  See "Performing the initial configuration" on page 22.
- If you do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 168.
- If the node was never configured with the `configure-console` command, proceed with the initial configuration.
  See "Performing the initial configuration" on page 22.

Next steps for a multi-node appliance

After the reimage is complete, do one of the following:

- If you reimaged only one of the nodes, remove the node from the appliance and then add it back to the appliance. If the node was previously updated, reinstall the update after you add it back.
  See "Removing a node" on page 171.
  See "Adding a node" on page 25.

- If you reimaged both nodes and want to delete the existing storage data, perform a storage reset and then perform the initial configuration again to reconfigure your settings.
  This option is not available if your appliance is in lockdown mode.
  See "Performing a storage reset" on page 170.
  See "Performing the initial configuration" on page 22.
- If you reimaged both nodes and do not want to delete the storage data, you can recover the appliance with the existing storage data.
  See "Recovering storage data after a factory reset or a reimage" on page 168.

Recovering storage data after a factory reset or a reimage

If you performed a factory reset or a reimage and want to keep the existing storage data, use the following procedure to recover the appliance.

Note: If you have a multi-node appliance, you only need to use this procedure if you performed a factory reset or a reimage on both nodes. If you only reset or reimaged one of the nodes, add that node back to the appliance. See "Adding a node" on page 25.

To recover the appliance

1. Make sure that no new storage has been attached to the appliance that was not added to the appliance before the factory reset or the reimage.
2. Log in to the Flex Appliance Shell. If you have a multi-node appliance and performed a factory reset on both nodes, log in to the node that you did not remove from the appliance. If you reimaged both nodes, select one of the nodes to perform this procedure on and log in to that node.
3. Run the following command to reconfigure the network:

   ```
   setup configure-network
   ```

   Follow the prompts to enter the host network information.

   Note: Make sure that you enter the same settings that were configured before the factory reset or the reimage.

   ---

4 Run the following command:

```
system appliance-recover
```

Warning: If you have a multi-node appliance, do not run the `system appliance-recover` command from both nodes.

5 Follow the prompts to recover the appliance.

Note: If the recovery fails, you must restart the node before you retry the recovery.

6 If you have a 5150 or a 52xx appliance, add the applications that you have instances of and the add-ons that are installed on them to the repository before you start the instances. See “Adding files to the repository” on page 81.

7 If you have a multi-node appliance, add the node that you did not recover back to the recovered appliance. See “Adding a node” on page 25.

8 If your appliance previously had security patches installed, reinstall them.

Note: If the Flex Appliance Console was open before the appliance reset and recovery, open a new session after appliance recovery.

Features that must be reconfigured after an appliance recovery

If any of the following features were previously configured on the appliance, note that the settings cannot be saved during a recovery. Make sure that you reconfigure them after the recovery.

- Personal API tokens

  Note: The previous tokens still appear after the recovery, but they are shown as **Invalid**. Reissue the tokens to continue using them.

- Predefined API tokens

  Note: The previous tokens still appear after the recovery, but they are shown as **Invalid**. Delete all invalid tokens and generate new ones.

See “Revoking access for external monitoring” on page 148.
See “Providing access for external monitoring” on page 147.

- The appliance metadata for single sign-on (SSO)
  After a recovery, the appliance metadata file changes. Copy or download the new file and upload it to your identity provider (IDP).
  See “Adding an IDP” on page 55.
- Multifactor authentication for the shell
  If multifactor authentication was previously configured, you are forced to reconfigure it the next time you log in to the shell.
- Remote replication with self-signed certificates
  If you have paired appliances that use self-signed certificates for communication, you must repair the connection after a recovery.
  See “Repairing a lost connection between paired appliances” on page 117.

Performing a storage reset

The purpose of a storage reset is to remove existing data and instances. In most cases, you should perform a storage reset after a factory reset or a reimage. Make sure that the factory reset or the reimage completed successfully on all appliance nodes before you begin a storage reset.

Storage reset is not available if your appliance is in lockdown mode.

Warning: If you have a multi-node appliance, resetting the storage from one node removes the data for both nodes.

To perform a storage reset

1. Log in to the Flex Appliance Shell. If you have a multi-node appliance and performed a factory reset on both nodes, log in to the node that you did not remove from the appliance. If you reimaged both nodes, select one of the nodes to perform this procedure on and log in to that node.
2. Run the following command:

   ```
   system storage-reset
   ```

3 Enter **yes** to continue, and then enter **DELETE DATA** to confirm.

Note: Do not perform any other tasks on the appliance until the `storage-reset` operation is complete.

4 Perform the initial configuration again from the same node to reconfigure the appliance.

Removing a node

Use the following procedure to remove a node from a multi-node Flex appliance.

Note: If your appliance is in lockdown mode, removing a node also removes the lockdown mode on that node. This change does not go into effect until you physically disconnect the removed node from the shared storage shelves.

To remove a node

1 From the Flex Appliance Console, make sure that there are no instances running on the node that you want to remove. Use the **System topology** page to view all of the running instances and relocate them as necessary.

2 Log in to the Flex Appliance Shell on the node that you want to keep in the appliance. Run the following commands and check which node the `infra_svc` and `rep_svc` services are running on:

```
support shell

hagrp -state | grep infra_svc

hagrp -state | grep rep_svc
```

3 If either service is running on the node that you want to remove, run the following command to move it to the other node:

```
system ha-service migrate service=<service> node=<node hostname>
```

Where <*service*> is either `infra_svc` or `rep_svc`, and <*node hostname*> is the hostname of the node that you do not want to remove.

Rerun the `support shell` > `hagrp -state` commands to check the status of the migration.

4 Once you have verified that the services are no longer running on the node that you want to remove, run the following command to remove it:

```
setup remove-node
```

Follow the prompts to remove the node.

Note: Do not perform any other tasks on the appliance until the `remove-node` operation is complete.

---

5 When the `remove-node` operation is complete, disconnect the removed node from the shared storage shelves.

6 If you plan to add this node back to the original appliance or use it in another Flex multi-node appliance, you must first perform a factory reset. See "Performing a factory reset" on page 159.

Viewing or resetting the storage shelf order on a 52xx appliance

The appliance hardware monitoring assigns IDs to the storage shelves to make sure that each one can be uniquely identified. If you remove or replace a storage shelf on a 52xx appliance, you need to reset the storage shelf order for proper monitoring. Use the following procedure to view or reset the shelf order.

To view or reset the storage shelf order

1 Log in to the Flex Appliance Shell.

2 Run one of the following commands:

- To view the storage shelf order: `support show-shelf-order`
- To reset the storage shelf order: `support reset-shelf-order`

Chapter 12

Troubleshooting guidelines

This chapter includes the following topics:

General troubleshooting steps

If you experience any issues with Flex Appliance, use the following steps as a guide to help you resolve the problem.

Table 12-1 Steps for troubleshooting Flex Appliance problems

Step	Action	Description
Step 1	Note the error message	Error messages are usually the vehicle for telling you something went wrong. If you receive an error message, first follow any troubleshooting steps that are listed in the message. Some error messages begin with a Unique Message Identifier (UMI) code. UMI codes consist of the letter V followed by a string of numbers in the following format: V-123-456-789. To find additional troubleshooting information for specific error messages, perform a search for the message or the UMI code on the Support website.

Table 12-1 Steps for troubleshooting Flex Appliance problems *(continued)*

Step	Action	Description
Step 2	Check the appliance monitoring information	If you cannot resolve the issue based on the error message, or if you don't see an error message in an interface but still suspect a problem, you can: ■ Use the hardware monitoring information to check for hardware errors. See "Viewing the hardware status" on page 141. ■ Run an appliance self-test. See "Viewing system data" on page 145. ■ Use the `support shell` command to access additional read-only information on the appliance.
Step 3	Gather information for Technical Support	If you cannot resolve the issue on your own, you may need to contact Technical Support for assistance. Before you contact Support, gather the following information: ■ Relevant error messages Record or take screen shots of any error messages you received, including the UMI code if applicable. ■ Data Collect logs Generate a Data Collect log package from the Flex Appliance Console. See "Gathering logs" on page 175. ■ Appliance serial number Locate and record the serial number of the appliance node. If you have a multi-node appliance, record the serial number of both nodes. For more information on locating serial numbers, see the *Product Description* guide for your particular appliance hardware. Also make sure that Call Home is enabled for maximum supportability.
Step 4	Contact Technical Support	Contact Technical Support from the Support website.
Step 5	If your appliance is in lockdown mode, you may need to unlock access for support	If your appliance is in lockdown mode, your representative may need an access key to unlock greater access to troubleshoot the issue. Support can generate this access key on their own, but if you prefer, you can also generate it from System Health Insights. The access key has a two-hour expiration period, so make sure that your support representative is ready to assist before you generate it. See "Unlocking access in lockdown mode" on page 174.

Unlocking access in lockdown mode

If your appliance is in lockdown mode and you need assistance from Technical Support, your representative may need an access key to unlock greater access to troubleshoot the issue. Support can generate this access key on their own, but if you prefer, you can also generate it from System Health Insights.

Warning: Improper use of the access key may result in rendering the node or the entire appliance unusable. The key should only be used for designated troubleshooting and system configuration changes under Support guidance.

Any unauthorized use is at your own risk, and you assume any liability for failures, defects, loss of data or security, or other issues that may result from such usage.

Refer to the *System Health Insights User Guide* for the procedure to generate the access key. It has a two-hour expiration period, so make sure that your support representative is ready to assist before you generate it. You also need the node serial number. See "Locating the node serial number" on page 111.

Gathering logs

Logs provide support personnel detailed information about your appliance. You can share these logs with the Support team to resolve issues.

Note: You can only generate one log package at a time.

The following log packages are available on a Flex appliance:

- Appliance OS
  This log package includes the Flex Appliance software, high availability, and OS static logs.
  See the section called "Gathering appliance OS or Data Collect logs" on page 176.
- Data Collect
  This log package includes debugging information for the system. It provides a more complete view of the overall system status, which is helpful for technical support representatives.
  As part of a Data Collect package, you can also choose to include the following:
  - Application instance logs
    This option includes the logs for all instances that are running on the selected node.
  - Advanced logs
    These logs are helpful for storage and hardware failures.

  See the section called "Gathering appliance OS or Data Collect logs" on page 176.
- Performance
  This log package includes performance and configuration data from the appliance and the application instances.
  See the section called "Gathering performance logs" on page 176.

- Single application instance (NetBackup version 10.3.0.1 and later)
  You can also gather the logs for a single application instance. This option provides a faster way to collect the logs for a specific instance only.
  See the section called “Gathering logs for a single application instance” on page 177.

Gathering appliance OS or Data Collect logs

To generate and download an Appliance OS or Data Collect log package

1. From the Flex Appliance Console, click the question mark icon in the upper-right corner of the page, then select **Diagnostics**.
2. Click **Generate log package**.
3. By default, the logs mask user information such as hostnames, IP addresses, usernames, etc. The masking process adds additional time to the log collection. If you need to view the user information or want to speed up the log collection, deselect the **Enable data masking** option.
4. Select the node or nodes that you want to view logs for and the log type, then click **Generate**. Note that the Data Collect logs may take a long time to generate. When the operation is done, the generated log package appears in a table on the **Diagnostics** page.
5. To download the log package, select it in the table and click **Download**. A pop-up window appears that lets you limit the download bandwidth. Select this option if needed, then click **Download** to confirm.

Gathering performance logs

To generate and download a Performance log package

1. Log in to the Flex Appliance Shell and run one of the following commands:
   - To generate the log package immediately:
     ```
     support data-collect performance at=now
     ```
   - To generate the log package later:
     ```
     support data-collect performance at=<yyyy-MM-dd-HH:mm>
     ```
     Where *<yyyy-MM-dd-HH:mm>* is the year, month, day, hour, and minute when you want to generate the log package.
     For example, to collect the logs on August 3, 2023 at 6:30 P.M., run the following command:
     ```
     support data-collect performance at=2023-08-03-18:30
     ```

Note: You can only run or schedule one log generation at a time. To check if any log generations are already scheduled, use the `support data-collect list-job` command.

2 Depending on your environment, the logs take approximately one hour to generate. When they are ready, they appear in the table on the **Diagnostics** page of the Flex Appliance Console. To access this page from the console, click the question mark in the upper-right corner and select **Diagnostics**.

3 To download the log package, select it in the table and click **Download**. A pop-up window appears that lets you limit the download bandwidth. Select this option if needed, then click **Download** to confirm.

Gathering logs for a single application instance

Note: This procedure is available for NetBackup primary and media server instances on version 10.3.0.1 or later and for NetBackup WORM storage server instances on version 20.4 or later. The option to generate the log package still appears for earlier versions of NetBackup, but if you generate a package, it is empty.

To generate and download an instance log package

1 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.

2 Locate the instance that you want to gather logs for. If it is stopped, click **Actions** > **Start**.

3 Click **Actions** > **Generate log package**.

4 By default, the logs mask user information such as hostnames, IP addresses, usernames, etc. The masking process adds additional time to the log collection. If you need to view the user information or want to speed up the log collection, deselect the **Enable data masking** option.

5 Depending on your environment, the logs take a few minutes to generate. You can track the progress from the Activity Monitor.

When the instance logs are ready, they appear in the table on the **Diagnostics** page of the Flex Appliance Console. To access this page from the console, click the question mark in the upper-right corner and select **Diagnostics**.

Note: The instance logs are maintained for six hours after they are generated. After six hours, they are deleted.

Deleting logs

Use the following procedure to delete a generated log package.

To delete a log package

1. From the Flex Appliance Console, click the question mark icon in the upper-right corner of the page, then select **Diagnostics**.
2. Select the log package that you want to delete and click **Delete**. When the confirmation window appears, click **Delete** to confirm.