NetBackup and NetBackup Appliances Hardening Guide

Spring 2026

VERITAS
now part of Cohesity

NetBackup and NetBackup Appliances Hardening Guide

Last updated: 2026-06-24

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.

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Cohesity website:

https://sort.veritas.com/netbackup/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Cohesity community site:

http://www.veritas.com/community/

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/netbackup/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Top recommendations to improve your NetBackup and NetBackup appliances security posture

This chapter includes the following topics:

- Configuring a sign-in banner

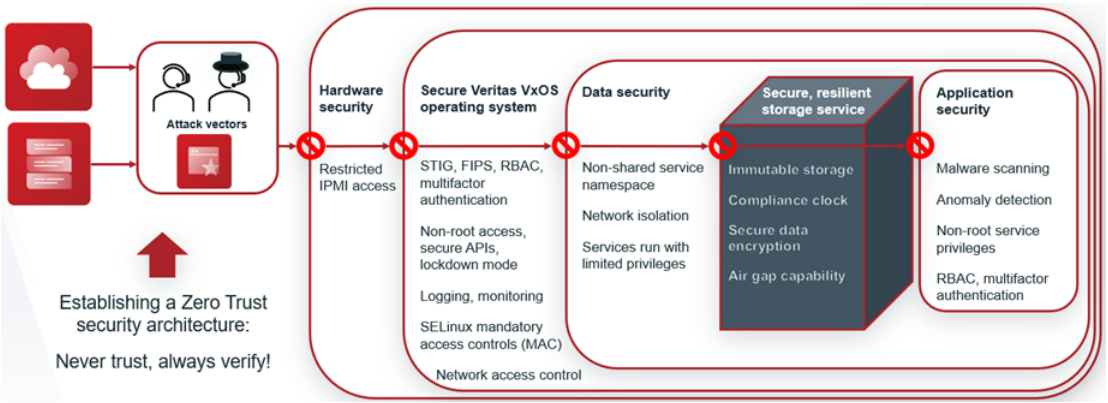
Introduction

NetBackup and NetBackup appliances bring together the power of NetBackup software with state-of-the-art servers and storage technology to create enterprise-class data protection with enhanced ransomware resiliency.

Ransomware attacks are on the rise. Intelligence channels increasingly show that attackers use stolen credentials to gain unauthorized access to backup software and appliances. The likelihood of a successful attack increases dramatically in the presence of out-of-date software, poor password management practices, generic user IDs, and the lack of multifactor authentication.

Figure 1-1 shows how these products use a multi-layered approach to protect against cyberattacks.

Figure 1-1 Multi-layered security



Cohesity highly recommends that you take advantage of the security features in our products to bolster your cybersecurity defenses, like multifactor authentication, lockdown mode, and immutability.

Do not put your critical backup data at risk. Follow the steps in this document to improve your NetBackup and NetBackup appliances security posture.

Keeping all systems and software updated

Cohesity delivers new releases and patches that add security features and address vulnerabilities. Register at the NetInsight Console SaaS portal to receive proactive

recommendations on product upgrades, such as security patches, hotfixes, and major or maintenance release updates.

The recommendations in this document apply to the following releases:

- Flex Appliance 7.0
- NetBackup Appliance 6.1
- NetBackup 11.1
- NetBackup Flex Scale 3.5
- Access Appliance 8.5

Links to the latest software releases:

- NetInsight Console
- Download Center
- NetBackup Automated Upgrades

Enabling multifactor authentication

Multifactor authentication uses at least two sources of verification to gain access to a resource. It is commonly used for activities like bank sign-ins and VPN access and can help you to align with your existing Identity and Access Management (IAM) policies.

NetBackup and NetBackup appliances provide multifactor authentication, which uses time-based one-time passwords to provide secure authentication.

You can also use single sign-on (SSO) and configure multifactor authentication through the SSO identity provider (IDP), or you can authenticate with smart cards or digital certificates.

How to enable multifactor authentication:

- Flex Appliance
  See “Managing multifactor authentication” on page 26.
  See “Managing multifactor authentication on a primary or a media server instance” on page 30.
  See “Managing multifactor authentication on a WORM storage server” on page 33.
- NetBackup Appliance
  See “Enabling multifactor authentication” on page 13.
- NetBackup
  See “About multifactor authentication” on page 92.

- NetBackup Flex Scale
  See “About multifactor authentication” on page 245.
- Access Appliance
  See “About multifactor authentication” on page 293.

How to enable single sign-on:

- Flex Appliance
  See “Managing single sign-on (SSO)” on page 34.
- NetBackup Appliance
  See “About single sign-on (SSO) authentication and authorization” on page 66.
- NetBackup
  See “Configure NetBackup for single sign-on (SSO)” on page 93.
- NetBackup Flex Scale
  See “About single sign-on (SSO) configuration” on page 249.
- Access Appliance
  See “About single sign-on (SSO) configuration ” on page 283.

How to enable smart cards or digital certificates:

- Flex Appliance
  See “Managing user authentication with smart cards or digital certificates” on page 35.
- NetBackup Appliance
  See “About authentication using smart cards and digital certificates” on page 69.
- NetBackup
  See “Configure user authentication with smart cards or digital certificates” on page 101.
- NetBackup Flex Scale
  See “Authenticating users using digital certificates or smart cards” on page 233.
- Access Appliance
  See “Configuring user authentication using digital certificates or smart cards” on page 286.

Enabling multiperson authorization

Multiperson authorization protects your environment from malicious acts by ensuring that a second authorized user approves a potentially undesirable action.

How to enable multiperson authorization:

- Flex Appliance
  Multiperson authorization is required by default to delete NetBackup application instances on versions 10.3.0.1 and 19.0.1 and later. It is also required for WORM storage server instances on version 19.0 in some scenarios. It cannot be disabled.
- NetBackup
  See "Workflow to configure multiperson authorization for NetBackup operations" on page 104.

This feature is not currently available for NetBackup Appliance.

Increasing the security level

By default, NetBackup appliances offer a hardened environment for protecting your infrastructure. Lockdown mode adds unique protection from credential compromise with its built-in One Time Password (OTP) mechanism, which prevents unauthorized access to the operating system.

NetBackup uses access codes for a similar purpose, to prevent unauthorized access to commands.

How to enable lockdown mode or access codes:

- Flex Appliance
- NetBackup Appliance
  See "Disable user access to the NetBackup appliance operating system" on page 74.
- NetBackup
  See "Access codes" on page 108.

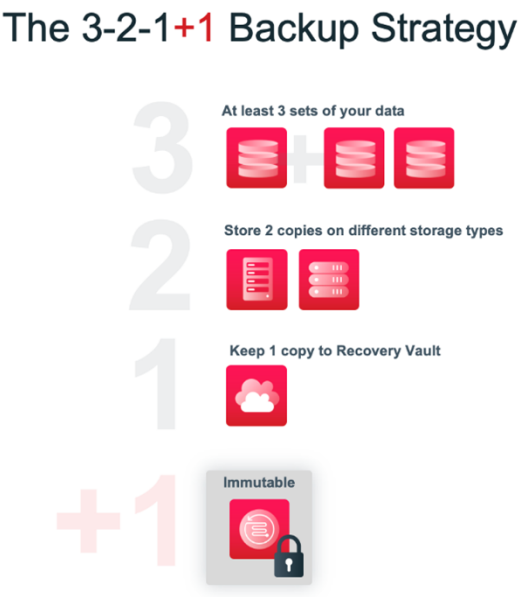
Implementing an immutable data vault

One of the best ways to safeguard your data is to implement immutable and indelible storage. This type of storage ensures that data cannot be changed, encrypted, or deleted for a determined length of time (or at all). NetBackup and NetBackup appliances provide secure and tamper-resistant immutable and indelible storage to protect data backups from being tampered with and from unauthorized access.

You can store immutable data in the cloud on object storage, including FortKnox for NetBackup or with third-party OpenStorage Technology (OST) vendors. FortKnox for NetBackup also creates a separation of duties where Cohesity manages the administration of the storage and provides you another layer of isolation from attack.

These features are vital to an effective and a rapid recovery strategy.

With the addition of immutability, Cohesity now recommends a new strategy for backups. In the past, the recommendation was a 3-2-1 strategy: three copies of data, two on site on different media, and one copy off site. The current rise in cyber threats calls for an extra "1," creating a 3-2-1+1 strategy: three copies of data, two on site on different media, one copy off site, and one copy that is immutable.



How to configure immutability:

- Flex Appliance
  See “Creating a NetBackup WORM storage server instance” on page 51.
- NetBackup
  See “Workflow to configure immutable and indelible data” on page 111.
- NetBackup Flex Scale
  See “Support for immutability in NetBackup Flex Scale” on page 225.
- Access Appliance
  See “Support for immutability in Access Appliance” on page 273.

This feature is not currently available for NetBackup Appliance.

Securing credentials

To avoid poor credential management practices, do not reuse or share passwords, and do not keep files of passwords on any systems. These practices create security, auditability, and compliance issues.

NetBackup and NetBackup appliances support external password management solutions. You can deploy CyberArk Privileged Access Management (PAM) solutions to enforce a password rotation policy and monitor all activity in privileged sessions.

How to configure an external password management solution:

- Flex Appliance and NetBackup Appliance
  Download the appliance plug-ins from the CyberArk marketplace.
- NetBackup
  See "Add a configuration for an external CMS server" on page 112.

Reducing network exposure

You can reduce your network exposure with the following features.

Network access control

Network access control can ensure that only authorized personnel can access selected networks or network segments to access backup administrative interfaces. For example, you can use an allowed list to control which IP addresses and subnets can access your appliances through SSH and HTTPS. All IP addresses that are not on the allowed list are blocked by default. This feature is an example of network segmentation and can prevent attackers from gaining system access.

How to configure network access control:

- Flex Appliance
  See "Using network access control" on page 48.
- NetBackup Appliance
  See "About Network Access Control" on page 75.
- NetBackup
  Network access control for NetBackup is available through the isolated recovery environment (IRE) feature. See the following section.

Isolated recovery environments

Another way to isolate and protect backups is to create an isolated recovery environment (IRE). NetBackup BYO and Flex Appliance include a turnkey, pull-based IRE that creates an air-gapped network environment. This feature lets you create

a vault for your data. Additionally, the proprietary compliance secure clock provides added confidence that your storage is never subject to time-based attacks that are meant to expire data prematurely.

How to configure an IRE:

- Flex Appliance
  See "Configuring an isolated recovery environment using the web UI" on page 56.
- NetBackup
  See "Configuring an isolated recovery environment on a NetBackup BYO media server" on page 114.
- NetBackup Flex Scale
  See "Configuring isolated recovery environment (IRE)" on page 256.
- Access Appliance
  See "Configuring an isolated recovery environment using the command line" on page 298.

Currently, NetBackup Appliance can be used for the production environment of an IRE but not as the target server.

Enabling encryption

Cohesity recommends that you enable data encryption at rest and in transit. Encryption prevents unauthorized data access and theft. If data is encrypted with robust industry standards, attackers cannot access it even if the data is stolen.

NetBackup software provides various options to configure encryption. To ensure optimal security, NetBackup includes encryption features for data at rest and in transit. You can encrypt your data before you send it to the cloud. You can use the built-in NetBackup key manager service (KMS) or configure NetBackup with a third-party KMS during storage server configuration.

Another way that your data is protected is with certificates, which create an encrypted connection between hosts. By default, NetBackup and NetBackup appliances use self-signed certificates for host communication. You can choose to configure external certificates instead. When you use external certificates, they are validated for authenticity by an external certificate authority (CA). In this way, the identity of the certificate holder is verified through a publicly known and trusted third party.

How to enable encryption:

- Flex Appliance
  Flex Appliance meets Federal Information Processing Standards (FIPS) 140-2 standards to keep data encrypted at rest and in transit. FIPS is enabled during the Flex Appliance installation process.

- NetBackup Appliance
  See “About data encryption ” on page 76.
  See “FIPS 140-2 conformance for NetBackup Appliance” on page 80.
- NetBackup
  See “About FIPS support in NetBackup” on page 122.
  See “Installing KMS” on page 128.
  See “Workflow for external KMS configuration” on page 132.
  See “Workflow to configure data-in-transit encryption” on page 136.
- Access Appliance
  See “FIPS 140-2 conformance for Access Appliance” on page 259.

How to configure external certificates:

- Flex Appliance
  See “Using an external certificate” on page 49.
- NetBackup Appliance
  See “About implementing external certificates” on page 83.
- NetBackup
  See “Workflow to use external certificates for NetBackup host communication” on page 161.
- NetBackup Flex Scale
  See “Deploying external certificates on NetBackup Flex Scale” on page 237.
- Access Appliance
  See “About external certificates on Access Appliance” on page 279.

Enabling catalog protection

Cohesity recommends that you protect NetBackup catalogs with dedicated policies for disaster recovery purposes. Failure to back up the NetBackup primary catalog may result in lengthy reconstruction activities in the event of a site disaster, hardware failure, or malicious attack. Two critical components should be protected: the NetBackup primary server catalog and the Media Server Deduplication Pool (MSDP) catalog.

For immutable storage, you can also create shadow copies of the catalog with the deduplication shell.

How to enable catalog backups:

- Flex Appliance
  For primary and media server instances, follow the same steps as NetBackup.
  See “Protecting the MSDP catalog on a WORM storage server” on page 60.

- NetBackup Appliance
  Follow the same steps as NetBackup.
- NetBackup
  See "Guidelines for managing the primary server NetBackup catalog" on page 190.
  See "About protecting the MSDP catalog" on page 192.

Enabling malware scanning and anomaly detection

Malware and ransomware programs may go undetected on the server and the storage system for days, weeks, or months. These long durations make it possible that the malware may be backed up along with the regular backups if existing antivirus and antimalware tools miss the signature. In a ransomware event, the best practice is to scan backups before recovery to find and eliminate malware before it is restored. To plan ahead before an actual cyber event, you can implement anomaly detection and malware scanning against production backups.

NetBackup provides unique built-in anomaly detection and malware scanning to help detect malware and ransomware early. Once malware scanning is enabled, make sure that critical events are sent to a security information and event management (SIEM) system for alerts and security incident orchestration through platforms like Service Now.

NetBackup Appliance additionally provides antimalware protection for the appliance OS.

Note: NetBackup appliances do not support the installation of third-party antivirus software, including on application instances.

How to enable malware scanning and anomaly detection:

- Flex Appliance
  Follow the same steps as NetBackup.
- NetBackup Appliance
  Follow the same steps as NetBackup and also enable antimalware protection for the appliance OS.
  See "About antimalware protection" on page 86.
- NetBackup
  See "How to set up malware scanning" on page 198.
  See "About backup anomaly detection" on page 200.

Enabling security observability

To detect and prevent threats, organizations need to promptly spot malicious insiders, compromised accounts, malware infections, and other problems. With NetBackup and NetBackup appliances, you can forward logs to an external log management server or a security information and event management (SIEM) solution. The logs include elevated shell commands for the appliances and have consistent timestamp formats, which are necessary for accurate and efficient event correlations and log analysis.

SIEM, SOAR, and XDR platforms are tools to combat unwanted trends and unsanctioned actions in IT ecosystems. NetBackup audit messages can be custom filtered and consumed by SIEM platforms, which scan the system log of the primary server and digest that information to provide reports, insights, and alerts. Automated response integration within NetBackup can automatically pause clients to stop any spread of undesired data, and SOAR integrations allow further customized actions based on scenarios in the various message categories. NetBackup adds more capability to your ransomware response plans with the insight and control of audit messaging.

How to enable log forwarding:

- Flex Appliance
  See “Forwarding logs” on page 51.
- NetBackup Appliance
  See “About forwarding logs to an external server” on page 86.
- NetBackup
  See “Send audit events to system logs” on page 208.
  See “Send audit events to log forwarding endpoints” on page 208.
- Access Appliance
  See “Forwarding logs to an external server” on page 308.

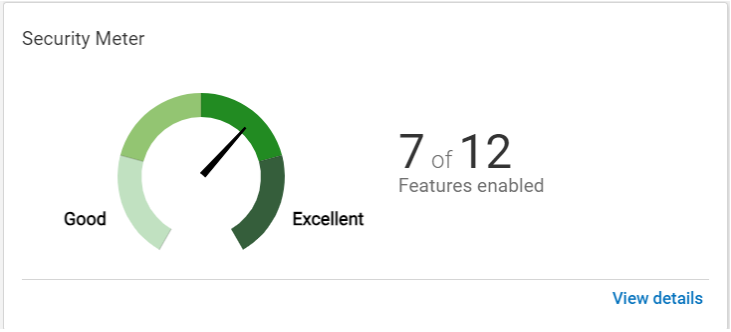
Flex Appliance also includes a security meter to view and configure the security settings from one location. The security meter tracks the security settings and shows you a list of the available features with quick links to configure them. It is accessible from the Flex Appliance Console home page by a security administrator.

Figure 1-2 shows how the security meter works, or you can see it in action in the security meter demo.

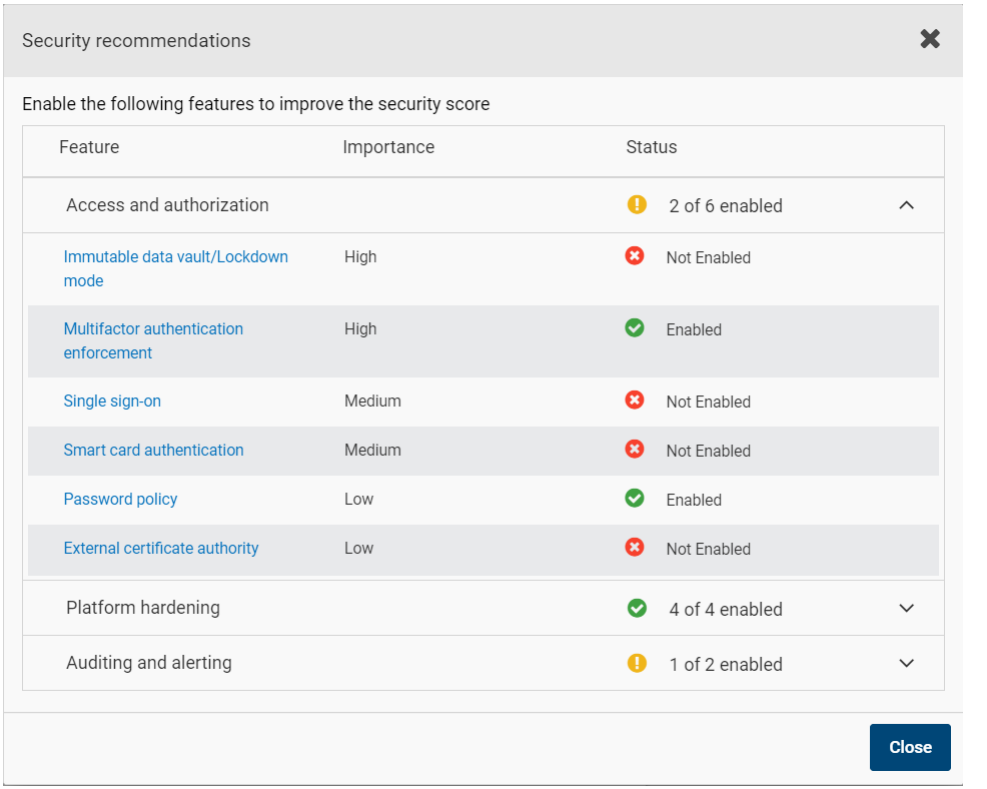
Figure 1-2 Security meter

The Access Appliance includes a security meter to view and configure the appliance security settings from one location. The security meter provides security insights and recommendations to improve the appliance security. The security meter keeps a track of the security settings and shows you a list of available security features with quick links to configure them. The security meter displays the current security index from good to excellent based on how many security features are turned on. Built-in security features are turned on and shown as **Enabled** in the security meter.

The security meter can be found on the appliance dashboard. Only an administrator user can view and manage the settings from the security meter. The following figure shows the security meter that is shown the appliance dashboard:



The following figure shows the available security settings that you can track and manage:



Restricting user access

NetBackup and NetBackup appliances support local users and remote users from Active Directory and LDAP user domains, who you can add as individual users or as user groups. As a best practice, you should only add those users or groups who need access to the system and restrict access from those who do not.

Note: When you connect a remote user domain to a Flex Appliance application instance, all users on the domain can log in to the instance. You must perform additional steps to restrict access to specific users or groups. For details, see the topics “Connecting an Active Directory user domain to a primary or a media server instance” and “Connecting an LDAP user domain to a primary or a media server instance” in the *NetBackup Application Guide*.

Configuring a sign-in banner

A sign-in banner is a customized text banner that appears every time that a user signs in to a product. You can use a sign-in banner to communicate important information to users. For example, a banner may include a security policy or a warning that they are on a restricted system and that all activity is logged.

How to configure a sign-in banner:

- Flex Appliance
  See “Using a sign-in banner” on page 61.
- NetBackup Appliance
  See “Creating the appliance login banner” on page 88.
- NetBackup
  See “Display a banner to users when they sign in” on page 209.
- Access Appliance
  See “Managing the login banner using the UI” on page 263.

Chapter 2

Steps to protect Flex Appliance

This chapter includes the following topics:

About Flex Appliance hardening

This chapter contains information on the Flex Appliance features that can help to secure your data protection infrastructure.

The following features are enabled by default:

- Intrusion detection and prevention through Security-Enhanced Linux (SELinux)
- Conformance to the OS hardening rules of the Security Technical Implementation Guides (STIGs).
- Conformance to the Federal Information Processing Standards (FIPS) 140-2.

Use the procedures in this chapter to enable other features to protect your appliance.

For more detailed information about Flex Appliance security, see the following guides:

- *Flex Appliance Getting Started and Administration Guide*
- *NetBackup Application Guide for Flex Appliance*
- *NetBackup Flex Appliance Security* white paper

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 27.

See “Enforcing multifactor authentication” on page 29.

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**.

Managing multifactor authentication on a primary or a media server instance

NetBackup primary and media server application instances support multifactor authentication for local, Active Directory (AD), and LDAP users. Multifactor

authentication uses time-based one-time passwords to provide secure authentication. Each user can configure multifactor authentication individually, or the **appadmin** user can enforce multifactor authentication for all users.

See "Configuring or disabling multifactor authentication on a primary server instance" on page 31.

See "Configuring or disabling multifactor authentication on a media server instance" on page 31.

See "Enforcing multifactor authentication on a primary or a media server instance" on page 32.

Configuring or disabling multifactor authentication on a primary server instance

For NetBackup primary server application instances, you can configure or disable multifactor authentication through the NetBackup web UI the same way that you would for any other primary server. Once you configure multifactor authentication, it is required for both the NetBackup web UI and for SSH access to the instance.

See the *NetBackup Web UI Administrator's Guide* for the steps to configure or disable multifactor authentication on a primary server instance.

Configuring or disabling multifactor authentication on a media server instance

Use the following procedures to configure or disable multifactor authentication on a NetBackup media server application instance.

Note: If multifactor authentication is enforced, users cannot disable it after the grace period.

To configure multifactor authentication on a media server instance

1. (Optional) If you have already configured multifactor authentication for another instance and want to use the same authenticator account to log in to this instance, run the following command on the other instance:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -show
   ```

   Take note of the key.

2. On the instance that you need to configure multifactor authentication for, run one of the following commands:

   - To enroll with a random key, run the following command:

```
/usr/openv/netbackup/bin/goodies/nbmfacfg -enroll
```

- To use an existing key, run the following command:

  ```
  /usr/openv/netbackup/bin/goodies/nbmfacfg -enroll -secret
  <existing key>
  ```

3. If you generated a new key, scan the QR code with an authentication app on your mobile phone. For example, Google Authenticator or Microsoft Authenticator.

   Note that the token validation is based on the server time. Ensure that the clock of the Flex Appliance and the mobile phone are correct.

Note: If the **appadmin** user becomes locked, they cannot reset multifactor authentication for themself. To avoid this situation, Cohesity recommends that two or multiple users scan the same QR code of the **appadmin** user with their mobile phones. If one user loses access to the token, another user can help them to enroll again.

To disable multifactor authentication on a media server instance

1. Log in to the instance as the user that you want to disable multifactor authentication for.
2. Run the following command:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -reset
   ```

Enforcing multifactor authentication on a primary or a media server instance

By default, multifactor authentication is optional. However, the **appadmin** user can enforce it for all users on the application instance.

Use the following procedures to enforce or stop enforcing multifactor authentication on a primary or a media server instance.

To enforce multifactor authentication on a primary or a media server instance

1. Log in to the instance as the **appadmin** user.
2. Run the following command:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -setenforce 1
   [-grace-period <days>]
   ```

   Where [-grace-period <*days*>] is an optional parameter to specify the number of days before users are forced to configure multifactor authentication before they can log in. If you do not include this parameter, the default of 90 days is used.

   For example:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -setenforce 1
   -grace-period 30
   ```

To stop enforcing multifactor authentication on a primary or a media server instance

1. Log in to the instance as the **appadmin** user.
2. Run the following command:

   ```
   /usr/openv/netbackup/bin/goodies/nbmfacfg -setenforce 0
   ```

Managing multifactor authentication on a WORM storage server

NetBackup WORM storage servers support multifactor authentication for local users. Multifactor authentication uses time-based one-time passwords to provide secure authentication. Each user can configure multifactor authentication individually, or the **msdpadm** user can enforce multifactor authentication for all users.

See "Configuring or disabling multifactor authentication on a WORM storage server" on page 33.

Configuring or disabling multifactor authentication on a WORM storage server

Use the following procedures to configure or disable multifactor authentication on a NetBackup WORM storage server.

Note: If multifactor authentication is enforced, users cannot disable it after the grace period.

To configure multifactor authentication on a WORM storage server

1. (Optional) If you have already configured multifactor authentication for another server and want to use the same authenticator account to log in to this server, run the following command on the other server:

   ```
   setting MFA show
   ```

   Take note of the key.

2. On the server that you need to configure multifactor authentication for, run one of the following commands:

   - To enroll with a random key, run the following command:

     ```
     setting MFA enroll
     ```

   - To use an existing key, run the following command:

     ```
     setting MFA enroll secret=<existing key>
     ```

3. If you generated a new key, scan the QR code with an authentication app on your mobile phone. For example, Google Authenticator or Microsoft Authenticator.

   Note that the token validation is based on the server time. Ensure that the clock of the Flex Appliance and the mobile phone are correct.

   Note: If the **msdpadm** user becomes locked, they cannot reset multifactor authentication for themself. To avoid this situation, Cohesity recommends that two or multiple users scan the same QR code of the **msdpadm** user with their mobile phones. If one user loses access to the token, another user can help them to enroll again.

To disable multifactor authentication on a WORM storage server

1. Log in to the server as the user that you want to disable multifactor authentication for.

2. Run the following command:

   ```
   setting MFA reset
   ```

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.

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.

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.

- The remote users who are associated with the smart cards or digital certificates must be imported to the appliance.
- Cohesity recommends that the appliance date and time are set using NTP.

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.

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.

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 that need multiperson authorization

The following operations require multiperson authorization:

- 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 2-1

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 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**.

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**.

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**.

Creating a NetBackup WORM storage server instance

NetBackup WORM (Write Once Read Many) storage server instances prevent your data from being encrypted, modified, or deleted. 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.

See the *NetBackup Administrator's Guide, Volume I* for more information about WORM storage.

Use the following procedure to create a NetBackup WORM storage server instance on Flex Appliance.

Note: Your appliance must be in lockdown mode before you can create a WORM storage instance.

See the topic "Changing the lockdown mode" in the *NetBackup Flex Appliance Getting Started and Administration Guide* for the steps to enable lockdown mode.

To create a NetBackup WORM storage server instance

1. Make sure that the NetBackup WORM storage server application you want to use is located in the repository.
2. Perform the following tasks if you have not already:
   - Configure at least one network interface. You can configure a physical interface, add a VLAN tag, or create a bond.
   - Add at least one tenant.
   - Verify that the appliance is in lockdown mode. You can check or change the lockdown mode from the **Lockdown mode** page on the Flex Appliance Console. See the topic "Changing the lockdown mode" in the *NetBackup Flex Appliance Getting Started and Administration Guide* for details.
3. Gather the following information for the new instance:

   Note: The hostname and IP address must not be in use anywhere else in your domain.

   - Tenant that you want to assign it to
   - Hostname (maximum of 63 characters including the domain name)
   - IP address
   - Network interface
   - Domain name
   - Name servers
   - Search domains
   - Primary server hostname (must be version 8.3.0.1 or later)
   - Media server hostname if applicable (must be version 8.3.0.1 or later)
   - Username for storage

NetBackup requires this username to connect to the deduplication storage. The username must be between 4 and 30 characters and can include uppercase letters, lowercase letters, and numbers.

- Password for storage
  NetBackup requires this password to connect to the deduplication storage. The password must be between 15 and 32 characters and must include at least one uppercase letter, one lowercase letter, one number, and one special character (_.+~={}?!).
- KMS key group
- KMS passphrase
- Certificate Authority (CA) information for one of the following:

  For a NetBackup CA:

  - CA SHA-1 or SHA-256 certificate fingerprint
    If the primary server is a Flex instance, you can locate this information from the instance details page of the primary server instance. Click on the instance name under **Application instances** on the **System topology** page.
    If the primary server is not a Flex instance, see the *NetBackup Security and Encryption Guide* for the steps to locate this information from NetBackup.
  - (Optional) Token for host ID-based certificate
    Depending on the primary server security level, the host may require an authorization or a reissue token. If you do not specify a token when you create the instance, the wizard attempts to automatically obtain the certificate.

  For an external CA:

  - Trust store, in PEM format
  - Host certificate, in PEM format
  - Private key, in PEM format
  - (Optional) Passphrase of the private key
    A passphrase is required if the key is encrypted.
- (Optional) Password for host name-based certificate
  A host name-based certificate is mandatory if Enhanced Auditing is enabled on the primary server. You can specify the password when you create the instance, or you can deploy the certificate from the primary server later.

4 On the primary server, use the `nbsetconfig` command or manually edit the NetBackup backup configuration file (`bp.conf` on Linux and UNIX, or the Windows registry) to add the following entry:

`MSDP_SERVER=<MSDP hostname>`

Where *<MSDP hostname>* is the hostname of the new WORM storage server instance.

5 If a firewall exists between the primary server and the new instance, open the following ports on the primary server to allow communication:

- `vnetd: 13724`
- `bprd: 13720`
- `PBX: 1556`
- If the primary server is a NetBackup appliance that uses TCP, open the following ports:
  443, 5900, and 7578.

6 From the **System topology** page of the Flex Appliance Console, navigate to the **Application instances** section.

7 Click **Create instance**.

8 Select the appropriate storage server application from the repository list that appears, making sure to verify the version number. Click **Next**.

9 Follow the prompts to create the instance. When you are done, you can view the progress in the Activity Monitor, which is accessible from the left pane of the Flex Appliance Console.

Note: If you use DNS and the DNS server includes both IPv4 and IPv6 addresses, the instance must be configured with both as well.

If you do not want to use DNS or want to bypass DNS for certain hosts, verify that the hostname resolution information is included in the **Hosts file entries** field. You must include entries for the primary server and any other NetBackup hosts that you want to communicate with the instance.

---

10 Once the instance has been created successfully, you must change the password from the known default password. To change the password, open an SSH session to the instance and log in with the following credentials:

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

Follow the prompt to enter a new password. When the password change is complete, you are logged out. You can log back in with the new password.

11 If you plan to create or already have multiple instances with deduplication storage, you must adjust the deduplication cache sizes so that the total memory of all instances does not exceed 75% of the physical RAM on the appliance.

The default cache sizes are as follows:

- `MaxCacheSize`: 512 MiB
- `MaxPredictiveCacheSize`: 40%
- `MaxSamplingCacheSize`: 20%

To tune the cache sizes on this instance:

- Run the following command to tune the `MaxCacheSize`:
  `setting set-MSDP-param max-cache-size value=<value>`
  Where <*value*> is the amount of the appliance RAM to use for the cache on the instance, as MiB, GiB, or a percent. For example, `value=1GiB` or `value=39%`.
- Run the following command to tune the `MaxPredictiveCacheSize`:
  `setting set-MSDP-param max-predictive-cache-size value=<value>`
  Where <*value*> is the amount of the appliance RAM to use for the predictive cache, as MiB, GiB, or a percent. For example, `value=1GiB` or `value=39%`.
- Run the following command to tune the `MaxSamplingCacheSize`:
  `setting set-MSDP-param max-sampling-cache-size value=<value>`
  Where <*value*> is the amount of the appliance RAM to use for the sampling cache, as MiB, GiB, or a percent. For example, `value=1GiB` or `value=39%`.
- Restart the `pdde-storage` process with the following commands:
  `sudo /etc/init.d/pdde-storage force-stop`
  `sudo /etc/init.d/pdde-storage start`

12 The appliance automatically creates a **PureDisk** storage server for the WORM storage instance that has the same name as the instance. Use the following steps to create a disk pool on that storage server:

From the NetBackup web UI, click **Storage**, click the **Disk pools** tab, and then click **Add**. Follow the prompts to configure the disk pool.

13 Use the following steps to create a deduplication storage unit for your instance:

From the NetBackup web UI, click **Storage**, navigate to the **Storage Units** tab, and then click **Add**. Follow the prompts and make sure that the **Enable WORM** option is activated.

You are ready to create a backup policy and start using your WORM storage instance. See the NetBackup documentation for more information.

Configuring an isolated recovery environment using the web UI

Perform the following steps to configure an isolated recovery environment using the NetBackup web UI.

Note: You can also configure and manage an IRE from the deduplication shell. See the *NetBackup Deduplication Guide* for more details.

Table 2-2 IRE configuration using the NetBackup web UI

Step	Task	Description
1.	Configure allowed subnets to allow only the hosts in the subnets to access the storage server.	See "Configuring the allowed subnets" on page 57.
2.	Configure reverse connections to support replicating backup images from storage servers outside the isolated recovery environment.	See "Configuring the reverse connections" on page 57.
3.	(Optional) Configure reverse replication schedule to allow network activities in a specific window.	See "Configuring the reverse replication schedule" on page 58.
4.	Configure SLP for replicating backup images from a production environment.	See "Adding a replication operation to SLP at the production primary server" on page 59.

Configuring the allowed subnets

Allowed subnets are like a firewall. Any hosts that are not in the allowed subnets has no access to the IRE MSDP server. Ensure that the IRE primary server is in the allowed subnets, otherwise you lose the control to the IRE MSDP server from the web UI. The computer you use to configure the IRE also must be in the allowed subnets.

To configure the allowed subnets

1. On the left, click **Storage > Disk storage**.
2. Click the **Storage servers** tab.
3. Click on the MSDP storage server that you want to configure.
4. Under **Isolated Recovery Environment** > **Allowed subnets**, click **Add subnet**.
5. Select **IPv4** or **IPv6** and type the IP address of the subnet and click **Add to list**.
6. Add all the subnets in the IRE domain that are required to access the MSDP server and click **Save**.

Configuring the reverse connections

Before you add reverse connections from the IRE storage server to production storage server, ensure that NBCA or ECA are configured on the IRE storage server for the production domain.

To configure the reverse connections

1. On the left, click **Storage > Disk storage**.
2. Click the **Storage servers** tab.
3. Click on the MSDP storage server that you want to configure.
4. Under **Isolated Recovery Environment** > **Reverse connections**, click **Add reverse connection**.
5. On the **Add reverse connection** page, provide the production primary server name.
6. Select the existing login credentials or add new credentials and click **Next**.
   - **Select existing credentials**: Select the existing credentials.
   - **Add a new credential**: Add a new credential for the production primary server. Under **Credential type**, select **Username Password authentication** or **Use API key**.

Note: The user of the production primary server needs privileges in the **default IRE SLP Administrator** role.

7 Click **Connect**.

8 On the next page, select **Remote MSDP storage server**.

You can select an MSDP storage server from the production domain. If the MSDP storage server has multiple network interfaces configured and you want the reverse connection, use another interface rather than the storage server name. You can type the FQDN of the network interface for the production MSDP storage server.

9 In the **Local interface** field, provide the local storage server interface name for data transmission.

If the IRE MSDP server has multiple interfaces and you want the IRE MSDP server to use a specific interface to connect to the production MSDP storage server, type the FQDN of the network interface for the IRE MSDP storage server.

If nothing is specified in **Local interface** field, IRE MSDP server uses the default network interface to connect to the production storage server.

10 Click **Add**.

A reverse connection is configured from the IRE MSDP server to the production MSDP server.

Configuring the reverse replication schedule

By default, an IRE MSDP storage server allows reverse connections to production storage server in a big window (24x7). For security purpose, administrator may want the reverse connections to be created in a small window.

To configure the allowed subnets

1 On the left, click **Storage > Disk storage**.

2 Click the **Storage servers** tab.

3 Click on the MSDP storage server that you want to configure.

4 Under **Isolated Recovery Environment** > **Reverse replication schedule**, click **Configure schedule**.

5 Configure the window for each weekday to allow reverse connections. Click the **Reset to default 24/7schedule** to restore the window to the default.

6 Click **Save**.

Adding a replication operation to SLP at the production primary server

To configure the reverse connections

1. On the left, click **Storage > Disk storage**.
2. Click the **Storage servers** tab.
3. Click on the MSDP storage server that you want to configure.
4. Under **Isolated Recovery Environment**, click **Modify SLP on the remote primary server**.
5. On the **Modify SLP on the remote primary server** page, provide the production primary server name.
6. Select the existing login credentials or add new credentials and click **Next**.
   - **Select existing credentials**: Select the existing credentials.
   - A**dd a new credential**: Add a new credential for the production primary server. Under **Credential type**, select **Username Password authentication** or **Use API key**.

     Note: The user of the production primary server needs privileges in the **default IRE SLP Administrator** role.
7. Click **Connect**.
8. Select the SLP that you want to add a replication operation to the IRE MSDP storage server and click **Next**.
9. Select an operation that you want to replicate to IRE MSDP storage server after the operation and click **Next**.
10. Select an SLP of the IRE domain for image import after replication completed.

11 On the **Window** tab, configure SLP window for the replication operation. Create a new SLP window or select an existing SLP window.

When you adjust the SLP window, ensure that the SLP window is covered by IRE schedule. If a replication is triggered outside the IRE schedule, reverse connection does not happen, and the replication job fails.

The **Synchronize with the reverse connection schedule** helps to replace the current SLP window with the IRE Schedule. You can adjust the SLP window based on the IRE Schedule.

The date and time that is shown on the page are based on the time zone of IRE primary server. If the production primary server and the IRE primary server are in different time zones, the time difference is calculated and the SLP window for the production primary server is converted automatically.

Click **Finish**.

12 Click **Save**.

All the configurations including MSDP storage server replication target, SLP window, and replication operation in the SLP are applied to the production primary server.

Protecting the MSDP catalog on a WORM storage server

By default, WORM storage servers store a copy of the MSDP catalog in the directory `/mnt/msdp/vol0` in addition to the original copy that is available under the dedicated catalog volume (`/mnt/msdpcat`).

If you want extra protection for the catalog, you can configure additional copies. Use the following procedures to manage the MSDP catalog copies from the deduplication shell.

To view the catalog copies

1 Open an SSH session to the server.

2 Run the following command:

```
cacontrol --catalog listshadowcopies
```

To configure an additional copy

1. Open an SSH session to the server.
2. Run the following command to determine which volumes exist in the `/mnt/msdp` directory:

   ```
   df -h
   ```

   Select one of the volumes other than vol0.

   Note: To configure an additional catalog copy, at least one volume other than vol0 must exist in the `/mnt/msdp` directory.

3. Run the following command:

   ```
   cacontrol --catalog addshadowcopy /mnt/msdp/<volume name>
   ```

   Where <*volume name*> is the volume that you chose in the previous step.

   For example:

   ```
   cacontrol --catalog addshadowcopy /mnt/msdp/vol1
   ```

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**.

Chapter 3

Steps to protect NetBackup Appliance

This chapter includes the following topics:

About NetBackup Appliance hardening

This chapter contains information on the NetBackup Appliance features that can help to secure your data protection infrastructure. For more detailed information about NetBackup Appliance security, see the *NetBackup Appliance Security Guide*.

About multifactor authentication

Starting with NetBackup Appliance release 5.3, multifactor authentication is supported.

Multifactor authentication requires users to verify their appliance login identity by means of a system-generated code that is required in addition to the standard login password. When multifactor authentication is enabled, each time you log in to the appliance you enter your username and password as usual. Next, you are prompted through a remote device, such as a smartphone, to enter a second factor to verify your identity. When you open the app on your smartphone, it shows a unique 6-digit code that you must enter to complete the login.

Note: You cannot use multifactor authentication if Smart Card configuration is enabled.

An administrator must configure their user account for multifactor authentication before other users can con configure their user accounts. Configuration for the feature is done from the following NetBackup Appliance Shell Menu view:

```
Main > Settings > Security > Authentication > MFA
```

For complete details and descriptions of the command options for this feature, see the *NetBackup Appliance Commands Reference Guide*.

After the first administrator has configured their user account for multifactor authentication, all of the following appliance users can configure their user accounts:

- Active Directory (AD)
- LDAP
- Local users
- NetBackup CLI users
- No-role users

Note: NetBackupCLI and no-role users must log in to the appliance and run the `multifactor-authentication` command, then run the available submenu commands. For complete details, see the `Settings > Security > Authentication > MFA` description in the *NetBackup Appliance Commands Reference Guide*.

First-time configuration for multifactor authentication

This section describes how an administrator configures their user account for multifactor authentication to allow all other users to configure their user accounts later.

Requirements for administrator configuration:

- Minimum of two administrator accounts - The appliance must have at least two administrator accounts before they can configure multifactor authentication for their user accounts. If only one administrator user account exists when another user tries to configure the feature, an error message appears to inform them to add another administrator user account.
- Minimum of one NTP server - At least one NTP server must be configured and added before the first administrator can configure multifactor authentication for their user account. A message appears if an NTP server is needed.

  Note: The NTP server is typically configured when you perform the initial configuration on the appliance. If you did not configure an NTP server at that time, you must log in to the appliance shell menu and configure at least one NTP server with the `Main > Network > NTPServer` command. For details, see the *NetBackup Appliance Commands Reference Guide*.

- After the above configurations are completed, all other appliance users can configure their user accounts.

The following procedure describes the first-time configuration for an administrator to configure their user account for multifactor authentication.

For first-time administrator user account configuration for multifactor authentication

1. Log in to the shell menu as an administrator with the following command:

   ```
   Main > Settings > Security > Authentication > MFA Configure
   ```

2. Follow the prompts to configure multifactor authentication for your user account.

3 After completing the previous steps, have another administrator log in to the appliance with the following command to configure their user account to use multifactor configuration:

```
Main > Settings > Security > Authentication > MFA Configure
```

4 To enforce multifactor authentication for all users of the appliance, run the following command:

```
Main > Settings > Security > Authentication > MFA Enforce
```

Note: You can run this command only after you have completed steps 1, 2, and 3.

Configure multifactor authentication for a user account

After the two required administrators have completed their user account configurations, all other appliance users can configure their user accounts.

Requirements for user configuration:

- If multifactor authentication is configured but not enforced for all users (global enforcement), a user can configure or unconfigure multifactor authentication for their account at any time.
- If multifactor authentication is configured and is also enforced for all users, a user can unconfigure multifactor authentication for their account only within a defined grace period. The grace period default is 90 days. After the grace period has expired, the user is forced to configure multifactor authentication during login, but they cannot unconfigure it.

To configure multifactor authentication for a user account

1 Log in to the appliance shell menu and run the following command to configure your user account for multifactor authentication:

```
Main > Settings > Security > Authentication > MFA Configure
```

For NetBackupCLI users and no-role users, log in to the appliance and run the `multifactor-authentication` command, then run the `Configure` submenu command.

2 Follow the prompts to configure multifactor authentication for your user account.

About single sign-on (SSO) authentication and authorization

You can configure SSO with a supported external identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Veritas product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- 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. ADFS (Active Directory Federation Services) is currently the only supported IDP for the NetBackup Appliance.
- IDP configuration is managed by using the `Main > Settings > Security > Authentication > SingleSignOn` command. You can configure only one IDP for SSO.
- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with SAML-authenticated users.
- SSO login is currently supported only to the NetBackup Appliance Web Console (web console).
- Global logout is not supported.

SSO configuration is supported from the NetBackup Appliance Shell Menu (shell menu). The following describes an overview on how to configure and enable SSO for an appliance.

Table 3-1 Process overview for SSO configuration

Step	Task	Description
1	Obtain the IDP metadata XML file.	The SAML metadata that is stored in XML files is used to share configuration information between the IDP and the appliance. The IDP metadata XML file is used to add the IDP configuration to the appliance. The following options are available: ■ Download the IDP metadata XML file from the service provider and upload it to the general share on the appliance. ■ Provide the URL address of the IDP metadata XML file for the appliance to download.
2	Configure SSO on the appliance.	Configure the appliance for SSO from the following shell menu view: `Main > Settings > Security > Authentication > SingleSignOn`
3	Authorize SSO users and user groups.	Configure appliance access for SSO users and user groups from the following shell menu view: `Main > Settings > Security > Authorization` You can grant administrator or AMS privileges to SSO users and user groups.

To perform the complete SSO configuration process, see the following topic:

See "Configure single sign-on (SSO) for a NetBackup Appliance" on page 67.

Configure single sign-on (SSO) for a NetBackup Appliance

The following procedure describes the complete process to configure an appliance for SSO.

To configure SSO on an appliance

1. Obtain the identity provider (IDP) metadata XML file by using one of the following methods:

   ■ Download
   Download and save the IDP metadata XML file from the IDP website. Then log in to the NetBackup Appliance Shell Menu (shell menu) and upload the file to the appliance by opening the general share as follows:

- Log in to the NetBackup Appliance Shell Menu (shell menu) and upload the file to the appliance by opening the general share as follows:
  `Settings > Share > General Open`

  Note: You can also upload the file into the general share directory from the **File Manager** tab in the NetBackup Appliance Web Console.

- URL
  Obtain the URL address of the IDP metadata XML file for the appliance to download. Make sure that it is a valid https address.

2 Configure SSO on the appliance as follows:

Note: You can configure only one IDP for SSO.

- Run the following command to add an IDP configuration to the appliance:
  `Settings > Security > Authentication > SingleSignOn Add`
- `idpname` - enter the name that you want to use for this IDP configuration.
- `metadata` - select how to associate the necessary metadata for the IDP configuration, as follows:
  Import: Import the IDP XML metadata file that you uploaded into the general share directory in the first step.
  URL: Enter the URL address of the IDP XML metadata file for the appliance to retrieve.
- *`userFieldName [userPrincipalName]`*
  `groupFieldName [memberOf]`
  These parameters are optional and are shown with their default values. You can change the default values as needed to retrieve the appropriate SAML assertion details.

After you have completed this step, the configuration is enabled by default.

3 Add authorized SSO user groups and users by running the `Settings > Security > Authorization` command. Use the following command options to authorize specific SSO user groups and users:

`Grant Administrator SSO_Groups` *`groups`*

`Grant Administrator SSO_Users` *`users`*

`Grant AMS SSO_Groups` *`groups`*

`Grant AMS SSO_Users` *`users`*

About authentication using smart cards and digital certificates

The following describes the supported interfaces for Smart Card Authentication.

2FA

Starting with appliance release 3.2, NetBackup supports two-factor authentication (2FA) for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Web UI.

Starting with appliance release 5.0, NetBackup appliances support two-factor authentication (2FA) for Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Appliance Web UI.

2FA for NetBackup Web UI

- The **nbasecadmin** user or any user with the NetBackup Adminstrator role can configure 2FA for the NetBackup Web UI.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.

2FA for NetBackup Appliance Web UI

Any user with the NetBackup Appliance administrator role can configure 2FA for the NetBackup Appliance Web UI. 2FA configuration requires configuring LDAP (with the directory type as OpenLDAP or ActiveDirectory) on the appliance.

For details about how to configure, enable or disable 2FA for the Appliance Web UI, see the following topic:

See “Smart card authentication for NetBackup Appliance Web UI” on page 71.

Smart card Authentication for NetBackup Web UI

The NetBackup Web UI supports authentication of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with a digital certificate or smart card, including CAC and PIV. This authentication method only supports one AD or LDAP domain for each appliance primary server domain and is not available for local domain users.

Note: Perform this configuration separately for each appliance primary server domain where you want to use this authentication method.

Ensure that you add the AD or the LDAP domain before you add access rules for domain users or configure the domain for smart card authentication. Use the `vssat` command to add AD or LDAP domains.

To add the AD or the LDAP domain for NetBackup

1. Log on to the appliance primary server as a NetBackupCLI user.
2. Run the `vssat` command.

   `vssat addldapdomain -d` *`DomainName`* `-s` *`server_URL`* `-u` *`user_base_DN`* `-g` *`group_base_DN`* `-t` *`schema_type`* `-m` *`admin_user_DN`*

   Replace the variables in the above command as per the following descriptions:

   - *`DomainName`* is a symbolic name that uniquely identifies an LDAP domain.
   - *`server_URL`* is the URL of the LDAP directory server for the given domain. The LDAP server URL must start with either `ldap://` or `ldaps://`. Starting with `ldaps://` indicates that the given LDAP server requires SSL connection. For example `ldaps://my-server.myorg.com:636`.
   - *`user_base_DN`* is the LDAP-distinguished name for the user container. For example, `ou=user,dc=mydomain,dc=myenterprise,dc=com`.
   - *`group_base_DN`* is the LDAP-distinguished name for the group container. For `example, ou=group,dc=mydomain,dc=myenterprise,dc=com`.
   - *`schema_type`* specifies which type of LDAP schema to use. The two default schema types that are supported are `rfc2307` or `msad`.
   - *`admin_user_DN`* is a string that contains the DN of the administrative user or any user that has search permission to the user container, or user subtree as specified by `UserBaseDN`. If the user container is searchable by anyone including an anonymous user, you can configure this option as an empty string. For example, `--admin_user=`. This configuration allows anyone to search the user container.
3. Verify that the specified AD or LDAP domain was successfully added using `vssat validateprpl`. Note that you can also use the `vssat` command with the following options:
   - `vssat removeldapdomain` removes an LDAP domain from the authentication broker.
   - `vssat validategroup` checks the existence of a user group in domain provided.
   - `vssat validateprpl` checks the existence of a user in domain provided.

For more details on the `vssat` command, see the *Veritas NetBackup Commands Reference Guide*

Smart card authentication for NetBackup Appliance Web UI

Ensure that you perform the following three steps before you perform authentication for the Appliance Web UI.

Note: You can perform the steps in any order.

1. Configure LDAP authentication with the directory type as OpenLDAP or ActiveDirectory.

   Settings > Security > Authentication > LDAP

2. Add and grant roles to LDAP users who will be authenticated by the appliance.

   Settings > Security > Authentication > LDAP > Users Add

   Settings > Security > Authorization > Grant

3. Add all the certificates in the CA chain to the appliance. Intermediate certificates on the card do not have to be added.

   Settings > Security > Certificates > AddCACertificate

The smart card command menu allows you to configure and display parameters related to the Appliance Web UI smart card authentication. You can also enable or disable this feature.

Settings > Security > Authentication > SmartCard

Table 3-2 Smart card menu commands

Command	Description
`Configure MappingAttribute`	The `Configure` command configures the appliance smart card authentication. It has one required and one optional configuration parameter. The `MappingAttribute` parameter specifies if the Common Name (CN) or the User Principal Name (UPN) of the certificate on the smart card is used to authenticate a user and determine that user's role. Enter CN or UPN. It is a required parameter. CN can be used if the CN in the certificates matches the CN field of the user records in the remote databases, OpenLDAP or ActiveDirectory. UPN can be used if the UPN in the certificates matches the UPN field of the user records in OpenLDAP or ActiveDirectory. When LDAP is, configured the `directoryType` is specified as OpenLDAP or ActiveDirectory.
`Configure OCSPURI`	The `OCSPURI` parameter (Online Certificate Status Protocol) determines if the certificate on the smart card has been revoked. It is an optional parameter. If present, this parameter overrides the OCSP URI present in the certificate. The URI is an FQDN or IPv4 address. An IPv6 address is not supported for the OCSP URI. **Note:** If authentication with smart card fails even after all the necessary steps have been performed, use the **SmartCard > Show** command and verify that the parameters, including the OCSP URI, if present, are correct. Verify that a name server which can resolve the OCSP URI is configured in the Network menu by navigating to **Network > DNS Show**
`Disable`	Disables smart card authentication.
`Enable`	Enables smart card authentication. You can enable smart card authentication only if LDAP has been configured, CA certificates have been added and smart card authentication has been configured.
`Show`	Displays a table which shows if smart card authentication is enabled, the selected mapping attribute, and the OCSP URI, if one was entered.

Smart card authentication for NetBackup Appliance Shell Menu

This topic provides the following information to configure smart card authentication for the NetBackup Appliance Shell Menu (shell menu):

- Order of steps
- Smart card SSH menu commands

Order of steps

1. Enable smart card authentication for SSH. You must first enable the feature before you can add the public key (step 3).
2. Configure the mapping attribute to determine which field in the remote database is used to search for the public key.
3. Add the public key for a local user. You can use either a public key file or a certificate file method.
4. (Optional) Choose to enable or disable password authentication for SSH login.

Table 3-3 Smart card SSH menu commands

Command	Description

`Configure MappingAttribute CN/UPN`
 	
`Configure PublicKey Add filetype <username>`
 	
`Configure PublicKey Remove <username>`
	The `Configure` command configures the appliance smart card authentication and is used to configure the following parameters:
	
	MappingAttribute is for either CN (Common Name) or UPN (User Principle Name). This attribute determines which of those fields in the remote database is used to search for the public key.
	
	`Configure PublicKey Add filetype <username>` adds a public key for a local user. Here, *filetype* is either `CertificateFile` or `PublickeyFile`. For `CertificateFile` configurations, copy and paste the certificate content directly. For `PublickeyFile` configurations, locate the public key in the certificate file and copy it, then paste it directly.
	
	Note: Before you can add a public key, you must first enable SSH smart card authentication with the `Enable` command described further below.
	
	`Configure PublicKey Remove <username> removes a public key for a local user.`

`Disable`	Disables smart card authentication for SSH user.
`Enable`	Enables smart card authentication for SSH users. If all the prerequisites for DNS and smart card configuration commands have been performed successfully, authentication with smart cards is enabled. **Note:** Before you can add a public key, you must first run this command to enable SSH smart card authentication.
`PWauth`	Enables or disables password authentication for SSH login.
`Show`	Shows the values of the mapping attribute and status of the smart card authentication.

Configure role-based access control

After adding the AD and LDAP domains for NetBackup, you can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure role-based access control for the NetBackup web UI. For more information about configuring RBAC for NetBackup Appliance users, see the *NetBackup Web UI Administrator's Guide*.

Configure authentication for a smart card or digital certificate for the NetBackup Web UI

You can use the `nbasecadmin` user to log on to the NetBackup web UI and configure authentication for a smart card or digital certificate. Refer to the *NetBackup Web UI Administrator's Guide* for steps on performing the following procedures required for the configuration:

- Configure NetBackup Web UI to authenticate users with a smart card or digital certificate.
- Edit the configuration for smart card authentication.
- Add a CA certificate that is used for smart card authentication.
- Delete a CA certificate that is used for smart card authentication.

Disable user access to the NetBackup appliance operating system

Depending on the security policies of your organization, you can choose to permanently disable user access to the NetBackup Appliance operating system (VxOS). You can disable user access to the VxOS by configuring its security level to `High`. Note that the following restrictions are permanently enforced in the appliance:

- Users cannot access the maintenance shell. The `Support > Maintenance` menu is not available in the shell menu.

Note: Only Veritas support personnel can be granted access to the maintenance shell to troubleshoot issues and manage operating system-related tasks.

To permanently disable user access to VxOS

1. To view the current security level of the VxOS, use the following command:

   ```
   Main_Menu > Settings > Security > SecurityLevel Show
   ```

   The VxOS can operate in either of the following security levels:

Security level	Description
`Optimal`	Access to VxOS is granted as per standard Veritas security policies. This is the default security configuration.
`High`	Access to VxOS is permanently disabled for all users.
`Maintenance`	Access to VxOS is temporarily granted to Veritas support personnel through the maintenance shell. The security level is automatically reverted to `High` after the maintenance activity is completed.

2. To permanently disable user access to VxOS, configure the security level to `High`. Use the following command:

   ```
   Main_Menu > Settings > Security > SecurityLevel High
   ```

   Note: After switching to the `High` security level, you cannot revert to the default (`Optimal`) security level unless you perform a factory reset of the appliance.

About Network Access Control

The Network Access Control feature lets you control which IP addresses (IPv4 or IPv6) are allowed to access the appliance. This feature is available through the NetBackup Appliance Shell Menu as follows:

```
Main > Settings > Security > NetworkAccessControl
```

The available command options are *AddIP*, *DeleteIP*, and *Show*.

Appliance access is allowed through HTTPS for the NetBackup Appliance Web Console or rest APIs, and through SSH for the shell menu. To permit access to a specific appliance, add the necessary client IP addresses to the allowed list for that appliance. Any client IP addresses that are not included in the allowed list cannot access the appliance. Any interface level restrictions are managed separately and are also appliance-specific.

For high availability (HA) setups, you must configure the `NetworkAccessControl` options on both appliance nodes and the configurations must match.

If your appliance is configured as an Appliance Management Server (AMS) or is an agent for an AMS, make sure that you add those IP addresses to the allowed list. The AMS must include the IP addresses of the agents, and the agents must include the IP address of the AMS.

For complete details, see the *NetBackup Appliance Commands Reference Guide*.

About data encryption

The NetBackup Appliance offers the following encryption methodologies to protect both data at rest and in flight:

- Transmits data in encrypted formats by using secure tunnels. These configurations can be made by client-side encryption and also replication. If these options are not used, once the data is transmitted from the appliance, the network infrastructure is used for securing data in flight.
- Starting with NetBackup Appliance version 3.0 (NetBackup version 8.0), MSDP provides AES encryption. If your environment uses encrypted MSDP, new incoming data gets encrypted with AES 128-bit (default) or AES 256-bit. For more information, see the following NetBackup documents:
  Veritas NetBackup Deduplication Guide
  Veritas NetBackup Security and Encryption Guide
- Supports encryption using NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. See "KMS support " on page 76.

KMS support

NetBackup Appliance supports encryption that is managed by NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. KMS is supported on primary and media server appliances. Regenerating the data encryption key is the only supported method of recovering KMS on an appliance primary server.

The following describes the KMS key features:

- Does not require an additional license.
- Is a primary server-based symmetric key management service.
- Can be administered as a primary server with tape devices connected to it or to another NetBackup Appliance.

- Manages symmetric cryptography keys for tape drives that conform to the T10 standard (such as LTO4 or LTO5).
- Designed to use volume pool-based tape encryption.
- Can be used with tape hardware that has built-in hardware encryption capability.
- Can be managed by a NetBackup CLI administrator using the NetBackup Appliance Shell Menu or the KMS Command Line Interface (CLI).

About the keys used under KMS

The KMS generates keys from passcodes or auto-generates keys. Table 3-4 lists the associated KMS files that hold the information about the keys.

Table 3-4 KMS files

KMS files	Description
Keystore file	The keystore file (`KMS_DATA`) contains all of the key group and key records, along with some metadata.
KPK file	The KPK file (`KMS_KPKF`) contains the KPK that is used to encrypt the ciphertext portions of the key records that are stored in the keystore file.
HMK file	The HMK file (`KMS_HMKF`) contains the HMK that is used to encrypt the entire contents of the keystore file. The keystore file header is an exception. It contains some metadata like the KPK ID and the HMK ID, which is not encrypted.

Configuring KMS

To configure KMS on an appliance primary server, you must log in as a NetBackupCLI user.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbasecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on managing role-based access control, see the *NetBackup Web UI Administrator's Guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user,

---

The following describes how to configure and enable KMS on an appliance.

To configure and enable KMS on an appliance

1. Log in to the appliance primary server as a NetBackupCLI user.
2. Enter into a restricted shell environment by using the `Command` command as follows:

   ```
   [nb-appliance.NBCLIUSER>]# Command
   ```

3. Authenticate your CLI access using the following steps:

   - Generate an access code by running the following command:

     ```
     #bpnbat -login -logintype webui -requestApproval
     ```

     Make a note of the access code that is displayed in the command window.
   - Sign in to the NetBackup web UI as a NetBackup Command Line (CLI) Admin user and approve the CLI access request by entering the access code that you generated earlier.
     Once the request is approved, you will see a confirmation message in the restricted shell command window.

   For more information about access key and approval requests, refer to the *NetBackup Security and Encryption Guide*.

4. Create an empty database using the `nbkms` command, as follows:

   ```
   [nbucliuser-!>]# nbkms -createemptydb
   ```

5. Start `nbkms`. For example:

   ```
   [nbucliuser-!>]# nbkms
   ```

6. Create a Key group. For example:

   ```
   [nbucliuser-!>]# nbkmsutil -createkg -kgname KMSKeyGroupName
   ```

7. Create an active key. For example:

   ```
   [nbucliuser-!>]# nbkmsutil -createkey -kgname KMSKeyGroupName
   -keyname KMS KeyName
   ```

Enabling KMS encryption for MSDP

Verify that KMS is configured and running on the primary server. You can then enable KMS encryption for MSDP on all of the media servers that are associated with the primary server.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbasecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on how to manage role-based access control, see the *NetBackup Web UI Administrator's guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user,

---

The following describes how to enable KMS encryption for MSDP on an appliance.

To enable KMS encryption for MSDP

1. Log in to the appliance media server as a NetBackupCLI user.
2. Change the following options in the order as shown:

   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSType --value=0`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSServerName --value=<primary server hostname`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSKeyGroupName --value=msdp`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KeyName --value=<KMS KeyName>`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSEnable --value=true`
   - `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=ContentRouter --option=ServerOptions --value=verify_so_references,fast,encrypt`

     Repeat this step on all media servers that are associated with the primary server.

3 Identify yourself to the system by logging on to the NetBackup web application. Run the following command:

```
sudo /usr/openv/netbackup/bin/bpnbat -login -loginType WEB

Authentication Broker: ApplianceHostname

Authentication Port: 0

Authentication Type: unixpwd

LoginName: Username

Password: Password
```

4 Ensure that the KMS is registered with NetBackup Web Service.

```
sudo /usr/openv/netbackup/bin/nbkmscmd -discoverNbkms
```

5 Stop and restart the NetBackup services with the following commands:

- `bp.kill_all`
- `bp.start_all`

6 To verify that KMS encryption for MSDP is enabled on the media server, run a backup job on the server, then run the following command:

```
crcontrol --getmode
```

FIPS 140-2 conformance for NetBackup Appliance

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for validating cryptography modules. The FIPS 140-2 standard specifies the security requirements for cryptographic modules and applies to both the hardware and the software components. It also describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

Note: For more information about the FIPS 140-2 standard and its validation program, click on the following links:

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

---

FIPS validation for Java

Starting with NetBackup Appliance 4.1, the FIPS 140-2 standard is enabled by default for all Java-based services. The FIPS validation is achieved by using SafeLogic's CryptoComply modules.

FIPS validation for MSDP, NetBackup and VxOS

Starting with NetBackup Appliance release 5.0, you can enable the FIPS 140-2 standard for MSDP, NetBackup and VxOS. The NetBackup Cryptographic Module, which is used by MSDP, NetBackup and VxOS, is FIPS validated.

Once FIPS for VxOS is enabled, the `sshd` uses the following FIPS approved ciphers:

- aes256-ctr
- aes256-gcm@openssh.com

Older SSH Clients are likely to prevent access to the appliance after FIPS for VxOS is enabled. Check to make sure that your SSH client supports the listed ciphers, and upgrade to the latest version if necessary. Default cipher settings are not typically FIPS-compliant, which means you may need to select them manually in your SSH client configuration.

You can enable the FIPS 140-2 standard for NetBackup MSDP, NetBackup and VxOS with the following commands:

- `Main Menu > Settings > Security > FIPS Enable MSDP`, followed by the maintenance password.
  Enabling or disabling the `MSDP` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you enable or disable this feature.

  Note: If you have upgraded from a previous version of NetBackup Appliance, ensure that you enable MSDP only after your existing data has been converted to use FIPS compliant algorithms. To check the current status of the data conversion use the `crcontrol --dataconvertstate` command. Enabling MSDP before the status is set to **Finished** can cause data restoration failures.

- `Main Menu > Settings > Security > FIPS Enable NetBackup`, followed by the maintenance password.
  Enabling or disabling the `NetBackup` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you enable or disable this feature.

- `Main Menu > Settings > Security > FIPS Enable VxOS`, followed by the maintenance password.
  Enabling or disabling the `VxOS` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable or disable this feature.
- `Main Menu > Settings > Security > FIPS Enable All`, followed by the maintenance password.
  Enabling or disabling the `All` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable or disable this feature.

Note: In a NetBackup Appliance high availability (HA) setup, you can enable the FIPS feature on both nodes only after you have completed configuration of the HA setup. The FIPS configuration must match on both the nodes. If FIPS is enabled on either node before the HA setup is completed, you must disable FIPS on that node before you complete the HA setup.

For complete information about FIPS commands, see the *NetBackup Appliance Commands Reference Guide*.

Limitations of FIPS mode

As FIPS security continues to increase, some older encryption methods can no longer be used.

When FIPS is enabled, appliance CIFS file share features work as follows: The appliance is added as a domain member in Active Directory (AD) environments with Kerberos authentication that uses AES ciphers.

CIFS shares opened by the following operations may not mount when using older authentication methods, like NTLM.

The following describes the impacted scenarios:

- For the general share:

  ```
  Settings> Share General Open
  Settings> LogForwarding > Share Open
  Manage> OpenStorage > Share Open
  Security> Certificate Import
  ```

- For incoming_patches:

  ```
  Manage> Software > Share Open
  ```

To work around these limitations, do one of the following:

- Disable the FIPS feature.
- Configure Active Directory authentication on the appliance. This adds the appliance as a domain member in Active Directory (AD) environments with Kerberos authentication that uses AES ciphers.

https://www.veritas.com/support/en_US/article.100054201

About implementing external certificates

NetBackup Appliance's web service uses the PKCS#12 standard and requires certificate files to be in the X.509 (`.pem`) format. If the certificate files are in the `.der`, `.DER`, or `.p7b` formats, NetBackup Appliance automatically converts the files to an accepted format.

Certificate requirements

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

- Certificate files are in the `.pem` file format and begin with "`-----BEGIN CERTIFICATE-----`".
- Certificate files contain the host name and FQDN in the subject alternative name (SAN) field of the certificate. If the certificate is used in an HA environment, the SAN field must contain VIP, host name, and FQDN.
- Subject name and common name fields are not empty.
- Subject fields are unique for each host.
- Subject fields contain a maximum of 255 characters.
- Server and client authentication attributes are set in the certificate.
- Only ASCII 7 characters are used in the subject and SAN fields of the certificate.
- The private key file is in the PKCS#8 PEM format and begins with `-----BEGIN ENCRYPTED PRIVATE KEY-----` or `-----BEGIN PRIVATE KEY-----`.

Certificate Signing Request (CSR)

Although optional, you can use the `Settings > Security > Certificate > CertificateSigningRequest > Create` command to generate a CSR. Copy the CSR content from the command line to your external certificate portal to obtain the required external certificate files.

```
Example:
Enter specified value or use the default value.
Common Name (eg, your name or your server's hostname) [Default abc123]:
Organizational Unit Name (eg, section) []:Appliance
Organization Name (eg, company) [Default Company Ltd]:YourCompanyName
Locality Name (eg, city) [Default City]:YourCity
State or Province Name (full name) []:YourStateorProvince
Country Name (2 letter code) [XX]:YourCountryName
Email Address []:email@yourcompany.com
Please enter the following 'extra' attributes
to be sent with your certificate request.
-----
A challenge password []:123456
An optional company name []:ABCD
Subject Alternative Name (DNS Names and/or IP Addresses comma separated):
abc123,def456.yourcompany.com
Subject Alternative Name (email comma separated):
Certificate Signing Request Name [Default abc123.csr]:
Validity period (in days) [Default 365 days]:
Ensure that the Distinguished Name (DN) is specified as a string consisting
of a sequence of key=value pairs separated by a comma:
Then the generated certificate signing request will be shown on the screen.
```

Register the external certificate

Starting from version 4.1, you can register an external certificate on both NetBackup Appliance and NetBackup using the `Settings > Security > Certificate > Import` command.

Perform the following steps to import the host certificate, host private key, and trust store to register the external certificate on NetBackup and NetBackup Appliance. Both NetBackup and NetBackup Appliance layers use the same host certificate, host private key, and trust store.

1. Log in to the appliance as an Administrator user.
2. From the NetBackup Appliance Shell Menu, run the `Settings > Security > Certificate > Import` command. The following NFS and CFS share locations are now accessible:
   - NFS: `/inst/share`
   - CFS: `\\<ApplianceName>\general_share`
3. Upload the certificate file, trust store file, and private key file to either of the share locations and enter the paths to the files.

4 Choose how to access the certificate revocation list (CRL). A CRL comprises a list of external certificates that have been revoked by the external certificate and should not be trusted. Select either of the following options:

- Use the CRL location provided in the certificate file.
- Provide the location of a CRL file (`.crl`) in the local network.
- Do not use a CRL.

5 Confirm the location of the certificate files you want to register on the appliance.

A detailed example of how to import the certificates is provided here.

- Identify the certificate which should be imported.
- Import the certificate.

```
Enter the certificate:
Enter the following details for external certificate configuration:
Enter the certificate file path: cert_chain.pem
Enter the trust store file path: cacerts.pem
Enter the private key path: key.pem
Enter the password for the passphrase file path or skip security
configuration (default: NONE):
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
2) Use the specific CRL directory.
3) Do not use a CRL.
q) Skip security configuration.
CRL option (1): 2
Enter the CRL location path: crl
Then confirm input information and answer the subsequent questions.
```

Adding and removing certificates

You can manage external certificates on NetBackup Appliance using the **Certificate** commands.

You can use the **Settings** > **Security** > **Certificate** > **Add CACertificate** command to add a server CA, HTTPS proxy CA, or LDAP CA certificate to the certificate authority list. Ensure that you paste the CA certificate content in the PEM or P7B format. The Appliance appends this CA certificate to the certificate authority list. Before appending the CA certificate, the appliance verifies whether the CA certificate is already being used on the appliance. If yes, the appliance quits with a message.

You can use the **Settings** > **Security** > **Certificate** > **Remove CACertificate** command to remove a server CA certificate from the certificate authority list. The

available CA certificates are listed and you can select the certificate that you want to remove.

About antimalware protection

Starting with software release 5.3, antimalware protection lets you manage the detection and removal of malware on the appliance. Feature configuration is available using the `Settings > Security > Antimalware` command from the NetBackup Appliance Shell Menu (shell menu).

The following describes the general feature functionality:

- Enable full malware protection on the appliance, which includes automatic protection (**AutoProtect**) and on-demand protection. The feature is enabled by default.**AutoProtect** protection scans all incoming files to the appliance. On-demand protection scans files that already exist on the appliance. You must set a daily or a weekly schedule to use on-demand protection.
- Set up a server to receive malware reports from the appliance. The LiveUpdate server is set as the default server.
- Manually generate a report that identifies the type of malware that was detected, the affected files, the severity level, and whether any files have been quarantined.
- Restore quarantined files that are not malware.

For complete configuration details, see the *NetBackup Appliance Commands Reference Guide*.

About forwarding logs to an external server

This feature can forward NetBackup Appliance system logs (syslogs) to an external log management server.

The following types of log severs are supported:

- Splunk

NetBackup Appliance uses the Rsyslog client to forward logs. In addition to Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance. Refer to the log management server documentation to verify Rsyslog client support.

You can view, enable, and disable log forwarding from the NetBackup Appliance Shell Menu.

See “Uploading certificates for TLS” on page 87.

See “Enabling log forwarding” on page 88.

Uploading certificates for TLS

Use TLS to secure the log transmissions from the appliance to the log server. TLS is optional for log forwarding. However, Veritas recommends that you enable TLS for security purposes.

NetBackup Appliance currently only supports the following:

- TLS Anonymous Authentication for log forwarding.
- X.509 file format for certificate files.

Before you enable TLS, you must first do the following:

- Deploy the configured certificate and private key files from the Certificate Authority (CA) server onto your log server.
- Upload valid certificates to opened NFS and CIFS shares on the appliance. For log forwarding security information, see the *NetBackup Appliance Security Guide*.

Note: You can also upload certificate files from the **Manage > File Manager** menu in the appliance web console.

To upload the certificate

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To open NFS and CIFS shares on the appliance, enter the following command:

   ```
   Share General Open
   ```
3. On the server where the certificates reside, mount an NFS or a CIFS share to the appliance as follows:

   NFS: `<appliance.name>:/inst/share`

   CIFS: `\\<appliance.name>\general_share`
4. Upload two certificates and one private key file. The certificate file names are as follows:
   - `ca-server.pem`
   - `nba-rsyslog.pem`
   - `nba-rsyslog.key`
5. To close the shares on the appliance, enter the following command:

   ```
   Share General Close
   ```

See "About forwarding logs to an external server" on page 86.

See "Enabling log forwarding" on page 88.

Enabling log forwarding

This procedure describes how to enable the log forwarding feature.

To enable log forwarding

1. Log on to the NetBackup Appliance Shell Menu and navigate to the `Main > Settings > LogForwarding` view.
2. To enable log forwarding, enter the following command:

   `Enable`

   Specify the following:

   - **Server name or IP address**: Enter the name or the IP address of the external log management server.
   - **Server port**: Enter the port number of the external log management server.
   - **Protocol**: Select either **UDP** or **TCP**. **TCP** is the default.
   - **Forward logs**: Select which types of logs to forward (OS, Appliance, AutoSupportClient, Infoscale). You can enter multiple log types with a comma-separated list.
   - **TLS**: Select either **Yes** or **No**. **Yes** is the default.

   Note: Enabling TLS requires that you upload two certificates and one private key to the appliance.

   See "Uploading certificates for TLS" on page 87.

   ---

3. Verify the configuration summary, and type `yes` to complete the configuration.

See "About forwarding logs to an external server" on page 86.

See "Uploading certificates for TLS" on page 87.

Creating the appliance login banner

The following procedures describe how to set the appliance login banner using the NetBackup Appliance Web Console.

To enable and create a new login banner using the NetBackup Appliance Web Console

1. Log onto the NetBackup Appliance Web Console.
2. Click **Settings > Notifications > Login Banner**.
3. Select the **Display Login Banner** check box.

   Note: The **Login Banner Heading** and **Login Banner Text** fields are only activated if **Display Login Banner** is checked.

4. Enter the desired text in the **Login Banner Heading** and the **Login Banner Text** fields.
5. Click **Preview** to review your changes.
6. Select the **Apply changes in NetBackup** check box if you want the same login banner to appear in the NetBackup Administration Console.
7. Click **Save**.

   When the confirmation dialog window appears, click **Yes** to apply the changes, or click **No** to continue making changes.

Once the login banner is enabled, you can go back and make changes. New changes are only applied if you click **Save**.

The following procedures describe how to set the appliance login banner using the NetBackup Appliance Shell Menu.

To enable and create a new login banner using the NetBackup Appliance Shell Menu

1. Log onto the NetBackup Appliance Shell Menu.
2. Run the `Main > Settings > Notifications > LoginBanner Set` command.
3. Enter a banner heading, and then press **Enter**.
4. Enter the banner message text.

   Once you have entered the banner message, type **end** on a new line and press **Enter**.

5 A preview of the login banner appears with the following message:

```
The existing login banner will be overwritten and the SSH daemon
will be restarted. Do you want to proceed? [y, n]: (y)
```

Type **y** and press **Enter** to set the login banner. Type **n** and press **Enter** to cancel any changes and exit the login banner configuration.

6 The following message appears:

```
Do you want to use this banner for the NetBackup Administration
Console as well? (Any existing Netbackup login banner will be
overwritten.) [y, n]: (y)
```

Type **y** and press **Enter** to set the login banner in the NetBackup Administration Console. Type **n** and press **Enter** to continue without changing the NetBackup login banner.

Once the login banner is enabled, you cannot make individual changes to it using the NetBackup Appliance Shell Menu. However, you can run the `LoginBanner Set` command again and overwrite the existing banner with one that contains your desired changes. Alternatively, you can use the NetBackup Appliance Web Console to make individual changes.

For more information on the login banner commands, refer to the *NetBackup Appliance Command Reference Guide*.

Chapter 4

Steps to protect NetBackup

This chapter includes the following topics:

- About backup anomaly detection
- Send audit events to system logs
- Send audit events to log forwarding endpoints
- Display a banner to users when they sign in

About NetBackup hardening

This chapter contains information on the NetBackup features that can help to secure your data protection infrastructure. For more detailed information about NetBackup security, see the *NetBackup Security and Encryption Guide*.

About multifactor authentication

Multifactor authentication is a multiple-step account login process that requires you to enter a 6-digit one-time password along with your password.

It is strongly recommended that you configure multifactor authentication to protect the security of your environment.

Note: User logins that are based on the following authentication types do not support multifactor authentication: SAML, smart card, and API keys.

See "Configure multifactor authentication for your user account" on page 92.

If multifactor authentication is configured, you may need to reauthenticate yourself by entering the one-time password that you see in the authenticator application on your smart device before you perform the following operations:

- Manage the global security settings for the primary server
- Adding an API key

If multifactor authentication is enforced in the NetBackup domain, all users must configure multifactor authentication for their user accounts for successful sign-in.

Configure multifactor authentication for your user account

For enhanced security, you can configure multifactor authentication for your user account. You must first install and configure authenticator application on your smart device that provides you with the one-time password.

Configuring multifactor authentication in NetBackup does not require internet connectivity on your smart device.

If the NetBackup administrator has enforced multifactor authentication in the NetBackup domain, you must configure it for your user account for successful sign-in.

To configure multifactor authentication for your user account

1. On the top right, click the profile icon and click **Configure multifactor authentication**.
2. On the **Configure multifactor authentication** screen, click **Configure**.
3. On the next screen, follow the given steps.

   Install and configure authenticator application on your smart device. It generates one-time password and sends it on your smart device.

   Supported authenticator applications
4. Scan the QR code with the authenticator application or enter the key manually.
5. Enter the one-time password that you see in the authenticator application on your smart device.
6. Select **Configure**.

   At the time of next sign-in, you need to enter the one-time password along with the username and password.

Enforce multifactor authentication for all users

Only the NetBackup administrator can enforce multifactor authentication for all NetBackup users.

To enforce multifactor authentication for all users

1. On the top right, click **Settings > Global security**.
2. On the **Security controls** tab, turn on **Enforce multifactor authentication**.

   Select **Confirm** to enforce multifactor authentication for all NetBackup users.

   Notify all users that they must configure multifactor authentication for their user accounts to be able to successfully sign in.

   See “Configure multifactor authentication for your user account” on page 92.

Configure NetBackup for single sign-on (SSO)

This section provides steps to set up trust and exchange configuration information between the IDP and the NetBackup primary server. Before proceeding with the steps, ensure that the following prerequisites are met in your environment:

- An IDP is set up and deployed in your environment.
- The IDP is configured to authenticate domain users of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP).

Table 4-1 Steps to configure NetBackup for single sign-on

Step	Action	Description
1.	Download the IDP metadata XML file	Download and save the IDP metadata XML file from the IDP. SAML metadata that is stored in XML files is used to share configuration information between the IDP and the NetBackup primary server. The IDP metadata XML file is used to add the IDP configuration to the NetBackup primary server.
2.	Configure the SAML keystore, and add and enable the IDP configuration on the NetBackup primary server	See "Configure the SAML KeyStore" on page 95. See "Configure the SAML keystore and add and enable the IDP configuration" on page 97.
3.	Download the service provider (SP) metadata XML file	The NetBackup primary server is the SP in the NetBackup environment. You can access the SP metadata XML file from the NetBackup primary server by entering the following URL in your browser: `https://primaryserver/netbackup/sso/saml2/metadata` Where *primaryserver* is the IP address or host name of the NetBackup primary server.
4.	Enroll the NetBackup primary server as a service provider (SP) with the IDP	See "Enroll the NetBackup primary server with the IDP" on page 100.
5.	Add SAML users and the SAML groups that use SSO to the necessary RBAC roles	SAML users and SAML user groups are available in RBAC only if the IDP is configured and enabled on the NetBackup primary server. For steps on adding RBAC roles, see the following topic.

After the initial setup, you can choose to enable, update, disable, or delete the IDP configuration.

After the initial setup, you can choose to update, renew, or delete the NetBackup CA SAML keystore . You can also configure and manage the ECA SAML keystore.

Configure the SAML KeyStore

To establish a trust between the NetBackup primary server and the IDP server, you must configure an SAML KeyStore on the NetBackup primary server. Depending on whether you are using the NetBackup CA or an external certificate authority (ECA), refer to either of the following sections:

Note: If you are using a combination of an ECA and NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server.

Note: The SAML KeyStore configuration using batch files, such as `configureCerts.bat`, `configureCerts`, `configureSAMLECACert.bat`, `configureSAMLECACert`and their corresponding options is deprecated.

Configure a NetBackup CA KeyStore

If you are using the NetBackup CA, create the NetBackup CA KeyStore on the NetBackup primary server.

To create a NetBackup CA KeyStore

1. Log on to the NetBackup primary server as root or administrator.
2. Run the following command:

   ```
   nbidpcmd -cCert -M master_server -f
   ```

   `-f` is optional. Use the option for the forceful update.

Once the NetBackup CA KeyStore is created, ensure that you update the NetBackup CA KeyStore every time the NetBackup CA certificate is renewed.

To renew the NetBackup CA KeyStore

1. Log on to the NetBackup primary server as root or administrator.
2. Run the following command:

   ```
   nbidpcmd -rCert -M master_server
   ```

3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

https://*primaryserver*/netbackup/sso/saml2/metadata

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

4 Upload the new SP metadata XML file to the IDP.

See "Enroll the NetBackup primary server with the IDP" on page 100.

To remove the NetBackup CA KeyStore

1 Log on to the NetBackup primary server as root or administrator.

2 Run the following command

```
nbidpcmd -dCert -M master_server
```

3 Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

https://*primaryserver*/netbackup/sso/saml2/metadata

Where *primaryserver* is the IP address or host name of the NetBackup primary server.

4 Upload the new SP metadata XML file to the IDP.

5 See "Enroll the NetBackup primary server with the IDP" on page 100.

Configure an ECA KeyStore

If you are using an ECA, import the ECA KeyStore to the NetBackup primary server.

Note: If you are using a combination of an ECA and the NetBackup CA in your environment, by default, the ECA is considered while establishing trust with the IDP server. To use the NetBackup CA, you must first remove the ECA KeyStore.

To configure an ECA KeyStore

1 Log on to the primary server as root or administrator.

2 Depending on whether you want to configure SAML ECA keystore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

- Run the following command to use NetBackup ECA configured KeyStore:
  `nbidpcmd -cECACert -uECA existing ECA configuration [-f] [-M primary_server]`

- Run the following command to use ECA certificate chain and private key provided by the user:

  ```
  nbidpcmd -cECACert -certPEM certificate chain file -privKeyPath
  private key file [-ksPassPath Keystore Passkey File] [-f] [-M
  <master_server>]
  ```

- Certificate chain file specifies the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
- Private key file specifies the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.
- KeyStore passkey file specifies the KeyStore password file path and must be accessible to the primary server on which the configuration is being performed.
- Primary server is the host name or IP address of primary server on which you want to perform SAML ECA KeyStore configuration. The NetBackup primary server where you run the command is selected by default.

To remove the ECA KeyStore

1. Log on to the primary server as root or administrator.
2. Download the new SP metadata XML file from the NetBackup primary server by entering the following URL in your browser:

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Where *primaryserver* is the IP address or host name of the NetBackup primary server.
3. Upload the new SP metadata XML file to the IDP.

   See "Enroll the NetBackup primary server with the IDP" on page 100.

Configure the SAML keystore and add and enable the IDP configuration

Before proceeding with the following steps, ensure that you have downloaded the IDP metadata XML file and saved it on the NetBackup primary server.

To configure SAML keystore and add and enable an IDP configuration

1. Log on to the primary server as root or administrator.
2. Run the following command.

   For IDP and NetBackup CA SAML KeyStore configuration:

```
nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
group field] [-cCert] [-f] [-M primary server]
```

Alternatively for IDP and ECA SAML KeyStore configuration:

Depending on whether you want to configure SAML ECA KeyStore using the configured NetBackup ECA KeyStore or you want to provide the ECA certificate chain and private key, run the following commands:

- Use NetBackup ECA configured keystore:

  ```
  nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
  file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
  user group field] -cECACert -uECA existing ECA configuration
  [-f] [-M Primary Server]
  ```

- Use ECA certificate chain and private key provided by the user:

  ```
  nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
  file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
  user group field] -cECACert -certPEM certificate chain file
  -privKeyPath private key file [-ksPassPath KeyStore passkey
  file] [-f] [-M primary server]
  ```

Replace the variables as follows:

- *IDP configuration name* is a unique name provided to the IDP configuration.
- *IDP XML metadata file* is the path to the XML metadata file, which contains the configuration details of the IDP in Base64URL-encoded format.
- `-e true | false` enables or disables the IDP configuration. An IDP configuration must be added and enabled, otherwise users cannot sign in with the single sign-on (SSO) option. Even though you can add multiple IDP configurations on a NetBackup primary server, only one IDP configuration can be enabled at a time.
- The SAML attribute names *IDP user field* and *IDP user group field* are used to map user identity information and group information in the Identity Provider. These fields are optional, and if not provided, they are mapped to the `userPrincipalName` and `memberOf` SAML attributes by default.

  For instance, if you have customized the attribute mapping in the Identity Provider to use attributes like email and groups, when configuring the SAML configuration, you need to provide the `-u` option for email and `-g` option for groups.

If you have not provided values for these attributes during configuration, ensure that the Identity Provider returns the values against the `userPrincipalName` and `memberOf` attributes.

For Example:

If SAML response is as follows:

saml:AttributeStatement <saml:Attribute Name="userPrincipalName"> <saml:AttributeValue>username@domainname</saml:AttributeValue> </saml:Attribute> <saml:Attribute Name="memberOf"> <saml:AttributeValue>CN=group name, DC=domainname</saml:AttributeValue> </saml:Attribute> </saml:AttributeStatement>

It implies that you need to map the `-u` and `-g` options against the fields "saml:Attribute Name".

Note: Ensure that the SAML attribute values are returned in the format of *username@domainname* for the field mapped to the `-u` option that defaults to `userPrincipalName`. If you include the domain name when returning group information, it should follow the format "(CN=group name, DC=domainname)" or "(domainname\groupname).

However, if you return the group name as plain text without domain information, it should be mapped without the domain name in the SAML RBAC group.

- *`primary Server`* is the host name or IP address of primary server to which you want to add or modify the IDP configuration. The NetBackup primary server where you run the command is selected by default.
- *`Certificate Chain File`* is the certificate chain file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.

  `Private Key File` is the private key file path. The file must be in PEM format and must be accessible to the primary server on which the configuration is being performed.

  `KeyStore Passkey File` is the KeyStore passkey file path and must be accessible to the primary server on which the configuration is being performed.

If your Identity Provider is already configured with SAML attribute names as `userPrincipalName` and `memberOf`, you do not have to provide the `-u` and `-g` option while configuration. If you are using any other custom attributes name, provide those names against `-u` and `-g` as follows:

For example:

If the Identity Provider SAML attribute names are mapped as "email" and"groups", use the following command for configuration:

```
nbidpcmd -ac -n cohesity_configuration -mxp file.xml -t SAML2 -e
true -u email -g groups -cCert -Mprimary_server.abc.com
```

`-u` and `-g` are optional and it depends on the Identity Provider configuration. Ensure that you specify the same parameter values that you have provided at the time of configuration.

Enroll the NetBackup primary server with the IDP

The NetBackup primary server must be enrolled with the IDP as a service provider (SP). For step-by-step procedures that are specific to a particular IDP, see the following table:

Table 4-2 IDP-specific steps for enrolling the NetBackup primary server

IDP name	Link to steps
ADFS	https://support.cohesity.com/s/article/article-100047744
Okta	https://support.cohesity.com/s/article/article-100047745
PingFederate	https://support.cohesity.com/s/article/article-100047746
Azure	https://support.cohesity.com/s/article/article-100047748
Shibboleth	https://www.veritas.com/docs/00047747

Enrolling an SP with an IDP typically involves the following operations:

Uploading the SP metadata XML file to the IDP

The SP metadata XML file contains the SP certificate, the entity ID, the Assertion Consumer Service URL (ACS URL), and a log out URL (SingleLogoutService). The SP metadata XML file is required by the IDP to establish trust, and exchange authentication and authorization information with the SP.

Mapping the SAML attributes to their AD or LDAP attributes

Attribute mappings are used to map SAML attributes in the SSO with its corresponding attributes in the AD or LDAP directory. The SAML attribute mappings are used for generating SAML responses, which are sent to the NetBackup primary server. Ensure that you define SAML attributes that map to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP directory. The SAML attributes must adhere to the following formats:

Table 4-3

Corresponding AD or LDAP attribute	SAML attribute format
`userPrincipalName`	***username@domainname***
`memberOf`	**(CN=*group name*, DC=*domainname*)**

Note: While adding the IDP configuration to the NetBackup primary server, the values entered for the user (`-u`) and user group (`-g`) options must match the SAML attribute names that are mapped to the `userPrincipalName` and the `memberOf` attributes in the AD or LDAP.

See "Configure the SAML keystore and add and enable the IDP configuration" on page 97.

Configure user authentication with smart cards or digital certificates

You can map a smart card or certificate with an AD or an LDAP domain for user validation. Alternatively, you can configure a smart card or certificate without an AD or an LDAP domain.

See "Configure smart card authentication with a domain" on page 101.

See "Configure smart card authentication without a domain" on page 103.

Configure smart card authentication with a domain

You can configure NetBackup to validate users with smart cards or certificates with an AD or an LDAP domain.

Note the following prerequisites:

- Before you add the authentication method you must add the domain that is associated with your NetBackup users. See the NetBackup Security & Encryption Guide.
- Ensure that you complete the role-based access control (RBAC) configuration for the NetBackup users before you configure smart card or certificate authentication.

To configure smart card authentication with a domain

1. Sign in to the NetBackup web UI.
2. At the top right, select **Settings > Smart card authentication**.
3. Turn on **Smart card authentication**.
4. Select the required AD or LDAP domain from the **Select the domain** option.
5. Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
6. Optionally, enter the **OCSP URI**.

   If you do not provide the OCSP URI, the URI in the user certificate is used.
7. Select **Save**.
8. To the right of **CA certificates**, click **Add**.
9. Browse for or drag and drop the **CA certificates** and click **Add**.

   Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

   Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or `PKCS #7` format and less than 64KB in size.
10. On the **Smart card authentication** page, verify the configuration information.

    After configuring smart card authentication, you must restart the NetBackup Web Management Console (nbwmc) service.
11. Before users 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 or contact your certificate administrator for more information.
12. When users sign in, they now see an option to **Sign in with certificate or smart card**.

    If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

    For such users, the domain name and domain type are smart card.

Configure smart card authentication without a domain

You can configure NetBackup to validate users with smart cards or certificates without an associated AD or LDAP domain. Only users are supported for this configuration. User groups are not supported.

To configure smart card authentication without a domain

1. At the top right, select **Settings > Smart card authentication**.
2. Turn on **Smart card authentication**.
3. (Conditional step) If AD or LDAP domain is configured in your environment, select **Continue without the domain** option.
4. Select a **Certificate mapping attribute**: Common name (CN) or Universal principal name (UPN).
5. Optionally, enter the **OCSP URI**.

   If you do not provide the OCSP URI, the URI in the user certificate is used.
6. Select **Save**.
7. To the right of **CA certificates**, click **Add**.
8. Browse for or drag and drop the **CA certificates** and click **Add**.
9. Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

   Certificate file types must be `.crt`, `.cer`, `.der`, `.pem`, or `PKCS #7` format and less than 64KB in size.
10. On the **Smart card authentication** page, verify the configuration information.

    After configuring smart card authentication, you must restart the NetBackup Web Management Console (nbwmc) service.

    Before users can use a digital certificate that is not installed on a smart card, the certificate must be uploaded to the browser's certificate manager.
11. When users sign in, they now see an option to **Sign in with certificate or smart card**.

    If you do not want users to have this sign-in option yet, turn off **Smart card authentication**. (For example, if all users do not yet have their certificates configured on their hosts.). The settings that you configured are retained even if you turn off smart card authentication.

Workflow to configure multiperson authorization for NetBackup operations

Here are the high-level steps to configure multiperson authorization for NetBackup operations:

Table 4-4

Step	Description
Step 1	Identify critical NetBackup operations that require multiperson authorization. See "NetBackup operations that need multiperson authorization" on page 105.
Step 2	Identify the approvers who can approve requests or multiperson authorization tickets.
Step 3	Assign the Default multiperson authorization approver RBAC role to the approvers. See "RBAC roles and permissions for multiperson authorization" on page 107.
Step 4	Configure multiperson authorization using the NetBackup web UI. See "Configure multiperson authorization" on page 107.
Step 5	When a user or a requester tries to perform an operation that requires multiperson authorization (for example, expiring an image), a ticket is generated. Initially, the ticket is in the pending state.
Step 6	The ticket is visible to all multiperson authorization approvers in the NetBackup web UI where they can review the ticket information and approve or reject the ticket.
Step 7	When the approver approves or rejects the ticket, the requester is notified. If the ticket is approved, the associated operation is executed. **Note:** For API key operations, the requester needs to execute the operation using the web UI after the ticket is approved.

Multiperson authorization configuration begins when the Administrator or the Security Administrator enables critical operations that require multiperson authorization and specifies other settings like expiration period and purge period.

A multiperson authorization configuration ticket is generated. After the approver approves the ticket, multiperson authorization configuration comes into effect.

Initial multiperson authorization configuration

Configuring multiperson authorization for the first time involves adding users to the Default multiperson Authorization Approver role. To start using the multiperson authorization for additional data security, the Security Administrator must enable the multiperson authorization for critical pre-defined operations that require an additional approval from a user with the Default multiperson Authorization Approver role.

Initially, the Security Administrator should configure multiperson authorization that results into a multiperson authorization ticket. After the approver approves the ticket, multiperson authorization becomes mandatory for the specified NetBackup operation (such as image expiry). The Administrator or Security Administrator can add users to the Default multiperson Authorization Approver role at any point in time.

NetBackup operations that need multiperson authorization

The following operations require multiperson authorization and therefore a ticket is generated for these operations:

- Configuring multiperson authorization
- Enabling and disabling operations that require multiperson authorization
- Adding exempted users
- Changing any multiperson authorization settings
- Expiring images
- Updating image expiration time
- Changing the MSDP WORM configuration
- Removing the MSDP WORM retention lock
- Removing hold applied on the images
- Updating CLI expiration period
- Adding, updating, and deleting an API key
- Adding, updating, and deleting KMS configuration, keys, and key groups
- Adding, updating, deleting malware scan host
- Adding, updating, deleting, copying backup and deployment policies
- Updating the following global security settings:

- Enabling and disabling NetBackup host communication with insecure hosts
- Adding host aliases with or without NetBackup administrator's approval
- Setting automatic deployment of certificates on a host
- Enabling and disabling CAC/PIV authentication
- Setting values for CAC/PIV certificate mapping attribute
- Setting the value of the CAC/PIV certificate mapping attribute that is used to perform a search in active directory
- Setting the value of the CAC/PIV certificate mapping attribute that is used to perform a search in LDAP directory
- Enabling and disabling AD/LDAP domain mapping
- Setting the value of the domain name that is used for user look-ups in active directory or LDAP
- Setting the value of the OCSP URI that is used for certificate revocation checks with respect to CAC/PIV authentication
- Enabling and disabling the data-in-transit encryption (DTE)
- Setting unique identifier for external certificates
- Allowing or disallowing the NetBackup web UI access to Operating System Administrators
- Allowing or disallowing the default CLI access to OS administrators
- Pausing client protection
- Pausing client image expiration
- Enabling and disabling TLS session resumption
- Enabling and disabling rule engine for anomaly detection
- Changing multifactor authentication configuration settings
- Setting audit retention period for audit report

Even if multiperson authorization is configured for image expiry, the following operations do not require multiperson authorization:

- Changing values for image retention level
- Modifying retention levels in policy and SLP
- Canceling incomplete SLPs using the `nbstlutil` command:
  Refer to the *NetBackup Commands Reference Guide*.

RBAC roles and permissions for multiperson authorization

multiperson authorization configuration requires the users to be assigned to the following RBAC roles:

- Administrator
- Default Security Administrator
- Default multiperson Authorization Approver

Users with these RBAC roles should have the following permissions.

Table 4-5

RBAC role	Permissions
Administrator	View, update multiperson authorization configuration, and delegate the configuration permissions to other users. View, update tickets, and delegate ticket permissions to other users.
Default Security Administrator	View, update multiperson authorization configuration, and delegate the configuration permissions to other users.
Default multiperson Authorization Approver	View and update tickets.
Default Operator	View all NetBackup entities.

Configure multiperson authorization

The configuration of multiperson authorization for NetBackup operations is supported only from the NetBackup web UI. A user with the Administrator or the Security Administrator role can configure multiperson authorization for critical NetBackup operations.

To configure multiperson authorization for NetBackup operations

1. On the left, select **Security > multiperson authorization**.
2. At the top right, select the option **Configure multiperson authorization**.
3. Go to **Operations for multiperson authorization**. Then select **Edit**.
4. Select all or any of the following critical operations for which you want to configure multiperson authorization.
   - Images

- Image expiry
- Remove image hold

- Security
  - Global security settings
  - Encryption key management
  - API keys

Note: If multiperson authorization is enabled for API key operations, a ticket is generated. After the multiperson authorization ticket is approved, the user needs to execute the ticket using the **Execute ticket** option in the NetBackup web UI and then the required API key operation is executed.

For NetBackup releases earlier than 10.5, if multiperson authorization is enabled, you cannot perform API key operations.

- MSDP WORM
  - WORM retention lock removal
  - WORM configuration change

5. Select **Save**.
6. Configure the users to be exempted from multiperson authorization.
7. Go to **Schedules**. Then select **Edit**.
8. Specify when you want to expire and purge the multiperson authorization tickets.
9. Select **Save**.
10. Select **Configure**.

Access codes

To run certain NetBackup administrator commands, for example `bperror`, you need to authenticate through the web UI. You need to generate an access code through the command-line interface, get the access request approved from the administrator, and then access the command.

With the web UI authentication for CLI access, NetBackup administrators can delegate the associated privileges to other users. By default, only a root administrator

or an administrator can perform NetBackup operations through the command-line interface. The web UI authentication support allows non-root users to administer NetBackup who have CLI access that the Security Administrator has granted. You can also administer NetBackup with a non-RBAC user role (such as Operating System Administrator) even though you are not registered as a NetBackup user. Each time you need to generate a new access code to access CLIs.

Request CLI access through web UI authentication

To run NetBackup commands using the NetBackup CLI, the following requirements exist for the user:

- The user must have the RBAC role Default NetBackup Command Line (CLI) Administrator or a role with similar permissions.
- The user must submit a request for temporary access to the CLI. By default, a CLI access session is valid for 24 hours.
  The command that the user runs for the request depends on whether or not they have access to the NetBackup web UI.
  See the section called “Request CLI access when you have access to the NetBackup web UI” on page 109.
  See the section called “Request CLI access from the security administrator” on page 110.

Request CLI access when you have access to the NetBackup web UI

If you have access to the NetBackup web UI, you can use the web UI to approve a CLI access request using the access code from the `bpnbat` command.

To request CLI access

1. Run the following command:

   ```
   bpnbat -login -logintype webui
   ```

   An access code is generated.
2. Open the NetBackup web UI.
3. On the top right, select the profile icon.
4. Select **Approve access request**.
5. Enter the CLI access code that was created when you ran the `bpnbat` command. Then select **Review**.
6. Review the access request details.

7 Select **Approve**.

8 After you approve the request, you can use the command-line interface to run the wanted commands.

Request CLI access from the security administrator

If you do not have access to the NetBackup web UI, you must submit a request for a CLI access to the security administrator. A user with the Default Security Administrator role or a role with similar permissions must approve the request.

To request CLI access from the security administrator

1 Run the following command:

```
bpnbat -login -logintype webui -requestApproval
```

An access code is generated.

2 Contact the security administrator and give them the access code to approve the CLI access request.

See "Approve the CLI access request of another user" on page 110.

3 After the request is approved, you can use the command-line interface to run the wanted commands.

Approve the CLI access request of another user

If you have the Default Security Administrator role or a role with similar permissions, you can approve the request of another user who needs CLI access. Note that to run commands, that user must also have the RBAC role Default NetBackup Command Line (CLI) Administrator or a role with similar permissions.

To approve the CLI access request of another user

1 The user that requires CLI access must first run the following command to request approval:

```
bpnbat -login -logintype webui -requestApproval
```

2 Sign in to the NetBackup web UI.

3 On the left, select **Security > Access keys**. Then select the **Access codes** tab.

4 Enter the CLI access code that you have received from the user who requires CLI access and select **Review**.

5 Review the access request details.

6 (Optional) Provide any comments.

7 Select **Approve**.

Workflow to configure immutable and indelible data

Carry out the following steps in the given order to protect your data by configuring immutability and indelibility.

Table 4-6 Workflow to configure immutable and indelible data

Step	Description
1	Configure the following WORM settings on the storage server. The storage administrator configures these settings outside of NetBackup. ■ **WORM capable** - If the storage unit and the associated disk pool are enabled to use the WORM property at the time of backup image creation, the backup images are set to be immutable and indelible. ■ **Lock Minimum Duration** - Specifies the minimum allowed duration for which the data for a backup image is indelible. The storage administrator sets this duration on the Logical Storage Unit (LSU) or the Domain Volume (DV), which NetBackup discovers. ■ **Lock Maximum Duration** - Specifies the maximum allowed duration for which the data for a backup image is indelible. The storage administrator sets this duration on the Logical Storage Unit (LSU) or the Domain Volume, which NetBackup discovers. Refer to the OST vendor plug-in documentation.
2	Configure a disk pool using WORM-capable volumes. See “About configuring disk pool storage” on page 111.
3	Configure a storage unit with the **Use WORM** option enabled. See “Use WORM setting” on page 112.
4	Configure a backup policy using the WORM-enabled storage unit. See “Creating a backup policy” on page 112.

Note: In case of storage changes or third-party OST vendor software upgrades, you need to manually update the storage servers and the disk pools. See the 'Completing your system update after an upgrade' section from the NetBackup Upgrade Guide.

About configuring disk pool storage

You can configure disk pools if you license a NetBackup feature that uses disk pools.

For more information, see the following guides:

- The *NetBackup AdvancedDisk Storage Solutions Guide*.
- The *NetBackup Cloud Administrator's Guide*.
- The *NetBackup Deduplication Guide*.
- The *NetBackup OpenStorage Solutions Guide for Disk*.
- The *NetBackup Replication Director Solutions Guide*.
- The *NetBackup Web UI Administrator's Guide*.

Use WORM setting

The **Use WORM** option is enabled for storage units that are WORM capable. Select this option if you want the backup images on this storage unit to be immutable and indelible until the WORM Unlock Time.

Note: You must also select the **On Demand Only** option whenever the **Use WORM** option is selected.

WORM is the acronym for Write Once Read Many.

Creating a backup policy

Use the following procedure to create a backup policy.

To create a policy

1. In the **NetBackup web UI**, select **Protections > Policies**.
2. Click **Add**.
3. Enter the policy name.
4. Configure the attributes, the schedules, the clients, and the backup selections for the new policy.

Add a configuration for an external CMS server

This section provides you the procedure for adding a configuration for an external CMS server.

To add a configuration for an external CMS server

1. On the left, click **Credential management**.
2. On the **External CMS servers** tab, click **Add** and provide the following properties:

- Configuration name
- Description (for example: This configuration is used to access the external CMS.)
- External CMS provider
- Host name
- Port number: Default port number 443 would be considered (if not provided by the user).

Note: While configuring the external CMS server for CyberArk server, user can use the DNS hostname or IPV4 address. However it is recommended to use the DNS hostname for connecting to the host. CyberArk configuration fails if IPV6 address is used.

---

3. Click **Next**.
4. On the Associate credentials page, **Select existing credential** or **Add a new credential**.

   More information is available on how to add a new credential.

   See "Add a credential for CyberArk" on page 113.
5. Click **Next** and follow the prompts to complete the wizard.

Add a credential for CyberArk

This type of credential allows you to access an external CMS server.

To add a credential for an external CMS server

1. On the left, click **Credential management**.
2. On the **Named credentials** tab, click **Add**.
3. Select **NetBackup** and click **Start**.

   On **Add a credential** page, provide the following properties:

   - Credential name
   - Tag
   - Description (for example: This credential is used to access the external CMS.)
4. Click **Next**.
5. Select **CyberArk** as the category.

6 Provide the credential details for CyberArk server:

These details are used to authenticate the communication between the NetBackup primary server and the external CMS server:

- Certificate - Specify the certificate file contents.
- Private key - Specify the private key file contents.
- CA Certificate - Specify the CA certificate file contents.
- Passphrase - Enter the passphrase of the private key file.
- CRL check level - Select the revocation check level for the external CMS server certificate.
  CHAIN - The revocation status of all the certificates from the certificate chain are validated against the CRL.
  DISABLE - Revocation check is disabled. The revocation status of the certificate is not validated against the CRL during host communication.
  LEAF - The revocation status of the leaf certificate is validated against the CRL.

7 Click **Next**.

8 Add a role that you want to have access to the credential.

- Click **Add**.
- Select the role.
- Select the credential permissions that you want the role to have.

9 Click **Next** and follow the prompts to complete the wizard.

Configuring an isolated recovery environment on a NetBackup BYO media server

You can configure an isolated recovery environment (IRE) on a NetBackup BYO media server to create an air gap between your production environment and a copy of the protected data. The air gap restricts network access to the IRE environment all the time. This feature helps to protect against ransomware and malware. To configure an IRE, you need a production NetBackup environment and a NetBackup IRE environment with MSDP server configured in a BYO Media server. The production environment does not require any additional steps for this feature.

Use the following procedure to configure an IRE on a BYO media server.

To configure an IRE on a BYO media server

1. Note that this procedure applies only to NetBackup 10.1 and later.

   Log in to the media server.

2. This step is optional. Use this step in any of the following conditions:

   - You want to enable IRE on an existing system.
   - AIR SLP is already configured.
   - You want to configure the IRE schedule in step 4 based on the existing SLP window.

   Run the following command to show the SLP windows for replication from the primary server to the MSDP storage on the media server:

   ```
   /usr/openv/pdde/shell/bin/show_slp_windows
   --production_primary_server production primary server name
   --production_primary_server_username production primary server
   username --ire_primary_server target primary server name
   --ire_primary_server_username target primary server username
   [--production_use_apikey] [--ire_use_apikey]
   ```

   Where:

   - The *production primary server name* is the fully qualified domain name (FQDN) of the primary server in your production environment.
   - The *production primary server username* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.
     The *production primary server username* must be in `domain_name\user_name` format on Windows.
   - The *target primary server name* is the FQDN of the primary server in the IRE. Use the same hostname that you used to configure the SLPs in the production environment.
   - The *target primary server username* is the username of a NetBackup user with permission to list the SLPs and storage units in the IRE environment.
     The *target primary server username* must be in `domain_name\user_name` format on Windows.

   For example:

   ```
   production_primary_server=examplePrimary.domain.com
   production_primary_server_username=appadmin
   ire_primary_server=exampleIREPrimary.domain.com
   ire_primary_server_username=appadmin
   ```

The following is an example output of the command:

```
EveryDayAtNoon: SLPs: SLP1 Sunday start: 12:00:00 duration: 00:59:59
Monday start: 12:00:00 duration: 00:59:59 Tuesday start: 12:00:00
duration: 00:59:59 Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59 Friday start: 12:00:00
duration: 00:59:59 Saturday start: 12:00:00 duration: 00:59:59
WeeklyWindow: SLPs: SLP2 Sunday start: 10:00:00 duration: 01:59:59
Monday NONE Tuesday NONE Wednesday NONE Thursday NONE Friday NONE
Saturday start: 10:00:00 duration: 01:59:59
```

This example shows two SLP windows:

- A daily window for one hour starting at noon.
- A weekly window for 2 hours starting at 10 A.M.

Note: If an SLP window is greater than 24 hours, the `show-slp-windows` may display the duration incorrectly.

3 Based on the output for your environment, determine a daily schedule that accommodates the SLP windows and take note of it. In the previous example, a daily schedule from 10 A.M. to 12:00 P.M. accommodates both SLP windows.

The start times in the output of this command are in the IRE server's time zone.

Note: If the time zone of the production primary server is changed, you must restart the NetBackup services.

4 Run the following command to configure the subnets and IP addresses that are allowed to access the media server:

```
/usr/openv/pdde/shell/bin/ire_network_control allow-subnets
--subnets CIDR subnets or IP addresses
```

Where the *CIDR subnets or IP addresses* field is a comma-separated list of the allowed IP addresses and subnets in CIDR notation.

For example:

```
/usr/openv/pdde/shell/bin/ire_network_control allow-subnets
--subnets 10.10.100.200,10.80.40.0/20
```

Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE environment must be included in the allowed list. If all these servers are in the same subnet, only the subnet is required to be in the allowed list.

Note: If your network environment is dual stack, ensure that both IPv4 and IPv6 subnets and IP addresses of the IRE domain are configured in allowed subnets. For example, if you specify only IPv6 subnets in the allowed subnet, all the IPv4 addresses are not allowed to access the IRE storage server.

5 Run the following command to set the daily air gap schedule:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time time --duration duration [--weekday 0-6]
```

`weekday` is optional. It starts from Sunday. You can configure different network and open or close window for a specific weekday. If it is not specified, the IRE schedule is the same on each day.

For example:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 10:00:00 --duration 03:00:00
```

Note: The SLP replication window on the production domain must be configured to be open at the same time as the IRE schedule. The IRE schedule window can be different for weekdays. You can configure a window for a specific weekday.

For example:

```
/usr/openv/pdde/shell/bin/ire_network_control set-schedule
--start_time 11:00:00 --duration 10:00:00 --weekday 0
```

Note: If the production and the IRE environments are in different time zones, the schedule must begin only once per day in both time zones.

For example, if one environment is in the Asia/Kolkata time zone and the other is in the America/New_York time zone, the following schedule in Kolkata is not supported: Tuesday start time 22:00:00 and Wednesday start time 03:00:00. When these start times are converted to the New York time zone, they become Tuesday start time 12:30:00 and Tuesday start time 17:30:00, which is not supported.

Note: If you want to open air gap network for 24 hours on all days, you do not need to configure IRE schedule. However, the IRE media server restricts the network access from the hosts that are not configured in the subnets that the air gap allows.

Configuring A.I.R. for replicating backup images from production environment to IRE BYO environment

Once IRE configuration is completed, the production NetBackup hosts are no longer able to access the IRE MSDP storage server. You need to enable MSDP reverse connection to allow the data transmission between the production MSDP server and the IRE MSDP server.

Note: A.I.R. configuration operations can be performed when the external network is open by IRE air gap. All the given operations are performed on the IRE MSDP server.

Prerequisites

Before you configure A.I.R. for replicating backup images from production environment to IRE BYO environment, ensure the following:

- In the case of NetBackup certificate authority (CA), get the CA certificate and host certificate for the IRE MSDP storage server from the production primary server.
- Create a token on the production primary server.

To configure A.I.R. for replicating backup images from production environment to IRE BYO environment

1. Run the following commands:
   - NetBackup certificate:

     ```
     /usr/openv/netbackup/bin/nbcertcmd -getCACertificate -server
     <production primary server>
     /usr/openv/netbackup/bin/nbcertcmd -getCertificate -server
     <production primary server> -token <token>
     ```

   - External certificate:

     ```
     /usr/openv/netbackup/bin/nbcertcmd -enrollCertificate -server
     <production primary server>
     ```

2. Run the following command to enable MSDP reverse connection.

   ```
   /usr/openv/pdde/shell/bin/ire_network_control reverse_connection
   --add production msdp server
   ```

3 This step is not required if you have not configured any IRE schedule. That is because if the IRE schedule is not configured, MSDP reverse connection is enabled for 24 hours on all days. The production primary server can configure the SLP replication operation with any SLP window.

Once the MSDP reverse connection is configured, copy the IRE schedule to the NetBackup production domain as an SLP window. Use the following command:

```
/usr/openv/pdde/shell/bin/sync_ire_window
--production_primary_server production primary server name
--production_primary_server_username production primary server
username [--slp_window_name slp_window_name ]
[--production_use_apikey]
```

Where:

The *production primary server name* is the fully qualified domain name (FQDN) of the primary server in your production environment.

The *production primary server username* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.

The *production primary server username* must be in `domain_name\user_name` format on Windows.

The *slp_window_name* is the name of the SLP window to be synced with the IRE window. It is an optional parameter. If the SLP window is not specified, an SLP window with the name `IRE_DEFAULT_WINDOW` is created on the production primary server.

4 You can then add the IRE MSDP storage server as a replication target of the production NetBackup domain. Then add the replication operation to an existing SLP to replicate from production NetBackup domain to IRE MSDP storage server using the following command:

```
/usr/openv/pdde/shell/bin/add_replication_op
--production_primary_server production primary server name
--production_primary_server_username production primary server
username --source_slp_name source slp name
--target_import_slp_name target import slp name
--production_storage_server production storage server name
--ire_primary_server_username ire primary server username
--target_storage_server target storage server name
--target_storage_server_username target storage server username
--production_storage_unit msdp storage unit name used in source
SLP [--slp_window_name slp window name] [--production_use_apikey]
[--ire_use_apikey]
```

Where:

The *production primary server name* is the fully qualified domain name (FQDN) of the primary server in your production environment.

The *production primary server username* is the username of a NetBackup user with permission to list SLPs and SLP windows in the production environment.

The *production primary server username* must be in `domain_name\user_name` format on Windows.

The *production storage server name* is the fully qualified domain name (FQDN) of the production storage server in your production environment.

The *ire primary server username* is the username for administrator user of IRE primary server.

The *ire primary server username* must be in `domain_name\user_name` format on Windows.

The *source slp name* is the SLP name on the production primary server against which a replication operation is added.

The *target import slp name* is the import SLP name from IRE primary server.

The *target storage server name* is the fully qualified domain name (FQDN) of the target MSDP storage server.

The *target storage server username* is the username of the target MSDP storage server.

The *slp_window_name* is the name of the SLP window that is synced with the IRE window. Alternatively, it is created on the production primary server before the operation. It is an optional parameter. If the SLP window is not specified, an SLP window with the name `IRE_DEFAULT_WINDOW` is used that must be created using the `sync_ire_window` command before the operation.

The *production_storage_unit* is the storage unit name of type PureDisk used in source SLP.

Note: The source SLP and target import SLP need to be created before the operation.

About FIPS support in NetBackup

By default, FIPS mode is disabled in NetBackup.

The following workloads are supported in FIPS-compliant mode:

- Oracle, MS-SQL, SAP HANA, DB2, VMware, Hyper-V, RHV, Nutanix, DynamicNAS, MongoDB, Hadoop, HBase, MySQL, PostgreSQL, SQLite, MariaDB, SharePoint
- Cassandra, Sybase, Informix, MS-Exchange, Enterprise Vault, BMR, Universal Shares, OpenStack (cloud-based solution)

The following operating system-level support is available in FIPS mode:

- Once you enable FIPS mode on RHEL 8, the operating system requires that each RPM package has a SHA-256 digest. RPMs that do not have this digest will fail to install. The RPMs that are built using the native toolchain present on RHEL 6 or RHEL 7 platforms do not include a SHA-256 digest and therefore can fail to install on RHEL 8 when FIPS mode is enabled. This issue affects NetBackup 9.1 and earlier setups as packages for these versions are built using the OS native toolchain on RHEL 7 or earlier.
  Starting with NetBackup 10.0, the packages are built using a toolchain that adds the SHA-256 digest and these can be installed on RHEL 8 with FIPS mode enabled.

The following components, configurations, or operations are not supported in FIPS mode:

- Client-side encryption

Note: To perform a backup with client-side encryption, you need to disable FIPS mode on the client host.

- NDMP backups
- Scripts (Perl, batch, shell, python) that are executed within NetBackup
- Binaries or utilities: `restore_spec_utility`, `nbcallhomeproxyconfig`, `nbbsdtar`, `nbrepo`
- NetBackup domain with NBAC enabled
  If NBAC is configured in the NetBackup domain, it is recommended that you do not enable FIPS mode.
- The MQBROKER processes do not support NetBackup-level FIPS configuration on Windows.
- MIT Kerberos used by Hadoop and HBase does not operate with a FIPS-enabled OpenSSL. To perform backup with Kerberos authentication, you need to disable FIPS on the backup host.
- NetBackup CloudPoint does not support the CloudPoint host that is configured in FIPS mode.
- SharePoint internally uses encryption algorithms that do not comply with FIPS standards. The Windows FIPS policy blocks the MD5 hashing algorithms that SharePoint uses. Therefore, the OS-level FIPS policy should be disabled for the SharePoint restores for successful operation.
  Note that NetBackup-FIPS is supported for protecting SharePoint.
  See the following articles for more details:
  FIPS and SharePoint Server
  SharePoint 2016 and FIPS

Enable FIPS mode on NetBackup during installation

NetBackup lets you enable FIPS mode during installation. For more information, refer to the NetBackup Installation Guide.

After you enable FIPS mode on NetBackup during installation, enable FIPS mode for the **NetBackup Administration Console**.

See “Enable FIPS mode for the NetBackup Administration Console” on page 126.

Enable FIPS mode on a NetBackup host after installation

This section provides steps to enable FIPS mode on a primary server, a media server, or a client in a NetBackup domain. You should do the following configurations on each host to enable FIPS.

If the host is a primary server, enable FIPS mode for the NetBackup Authentication Broker (AT) by updating the `VRTSatlocal.conf` configuration file on the primary server.

See "Enable FIPS mode for the NetBackup Authentication Broker service" on page 125.

To enable FIPS mode on a NetBackup host

1. Enable the `NB_FIPS_MODE` flag in the NetBackup configuration file.

   See "NB_FIPS_MODE option for NetBackup servers and clients" on page 127.

2. Restart the NetBackup services.

To verify if a certain daemon or a command runs in FIPS mode, check the respective logs. The log lines are available only for the daemons and commands that use cryptography.

Example 1: To verify if the `nbcertcmd` command runs in FIPS mode

1. Run the following command:

   ```
   nbcertcmd -ping
   ```

   Location of the command:

   Windows: *`install_path`*`\NetBackup\bin\nbcertcmd`

   UNIX: `/usr/openv/netbackup/bin/nbcertcmd`

2. Check the `nbcertcmd` logs.

   Location of the log directory:

   Windows: *`install_path`*`\NetBackup\logs\nbcert`

   UNIX: `/usr/openv/netbackup/logs/nbcert`

   The following log lines should be present:

```
<2> nbcertcmd: ./nbcertcmd -ping ProcessContext: ProcessName:[nbcertcmd],
FipsMode:[ENABLED], Username:[root], IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

Example 2: To verify if the NetBackup Web Management Console runs in FIPS mode

- By default, FIPS mode is disabled when the **NetBackup Web Management Console** (`nbwmc`) service runs. FIPS mode is enabled for the `nbwmc` service after you enable it for the NetBackup host.

  Check the `catalina` log file on the NetBackup primary server host to verify if the `nbwmc` service runs in FIPS mode.

  Location of the log file:

  Windows:
  `install_path``\NetBackup\wmc\webserver\logs\catalina-`*`date`*`.log`

  UNIX: `/usr/openv/wmc/webserver/logs/catalina-`*`date`*`.log`

  The following log lines should be present:

  ```
  The nbwmc service is running in FIPS approved mode
  ```

Enable FIPS mode for the NetBackup Authentication Broker service

The NetBackup Authentication Broker (`nbatd`) service runs only on the NetBackup primary server, therefore you need to enable FIPS mode on the primary server to enable it for the `nbatd` service.

FIPS mode is disabled by default.

Note: From version 10.5 and later, for Cloud Scale deployment, the `nbatd` containerized service is running in a separate Kubernetes Pod cluster server rather than the NetBackup primary server Pod. To enable the FIPS mode for the NetBackup Authentication Broker service, execute the same steps on the `nbatd` containerized service mentioned in the section *Enable FIPS mode for the NetBackup Authentication Broker service*.

To enable FIPS mode for the `nbatd` service or the `nbatd` containerized service

1. Open the following directory on the primary server:

   On UNIX: `/usr/openv/netbackup/sec/at/bin/`

   On Windows: *`install_path`*`\NetBackup\sec\at\bin\`

2. Run the following command:

   On UNIX:
   ```
   run vssregctl -s -f
   /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
   -b "Security\Authentication\Client" -k FipsMode -t int -v 1
   ```

   On Windows:
   ```
   run vssregctl -s -f
   "install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
   -b "Security\Authentication\Client" -k FipsMode -t int -v 1
   ```

   For example:

   Run the following command on Windows:

   ```
   vssregctl -s -f
   "Install_Path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
   -b "Security\Authentication\Client" -k FipsMode -t int -v 1 3
   ```

   Check the `nbatd` logs.

   Location of the `nbatd` logs:

   On UNIX:

   ```
   /usr/openv/logs/nbatd
   ```

   On Windows:

   ```
   install_path\NetBackup\logs\nbatd
   ```

   The following log lines should be present:

   ```
   *** Trying to start Broker In FIPS mode ***

   *** Broker In FIPS mode already ***
   ```

3. Restart the NetBackup services.

Enable FIPS mode for the NetBackup Administration Console

By default, FIPS mode for the **NetBackup Administration Console** is disabled.

To enable FIPS mode for the NetBackup Administration Console (on local or remote host)

1. Open the **NetBackup Administration Console** configuration file.
   - On Windows computers, the file containing configuration options for the **NetBackup Administration Console** is: `install_path\java\nbj.conf`
   - On UNIX computers, the file containing configuration options for the **NetBackup Administration Console** is: `/usr/openv/java/nbj.conf`
2. In the configuration file, enable the `NB_FIPS_MODE` option. Use the following format:

   ```
   NB_FIPS_MODE = true
   ```
3. Save the changes.
4. Restart the **NetBackup Administration Console**.

To verify if the NetBackup Administration Console runs in FIPS mode

- Check the **NetBackup Administration Console** logs.

  Log location:

  On Windows:
  `install_path\logs\user_ops\nbjlogs\jbp.root.jnbSA.`*`pid`*`.log`

  On UNIX: `/usr/openv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA.`*`pid`*`.log`

  On a standalone console, create a directory structure and check the logs.

  If the log file contains the following log lines, it means the console runs in FIPS mode:

  ```
  com.safelogic.cryptocomply.fips.approved_only: true
  ```

  It should have the following log lines:

  ```
  JavaPresentationLayer- FIPS mode enforced. Reconfiguring SunJSSE.
  JavaPresentationLayer- Administration console is running in FIPS approved
  ```

Note: This FIPS mode configuration does not affect the NetBackup KMS FIPS mode. NetBackup KMS continues to run in FIPS mode by default.

NB_FIPS_MODE option for NetBackup servers and clients

Use the `NB_FIPS_MODE` option to enable the FIPS mode in your NetBackup domain.

Table 4-7 NB_FIPS_MODE information

Usage	Description
Where to use	On NetBackup servers or clients.

How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	By default, the `NB_FIPS_MODE` option is disabled.
	To enable the option, use the following format:
	`NB_FIPS_MODE = ENABLE`
	To disable the option, use the following format:
	`NB_FIPS_MODE = DISABLE`

Equivalent NetBackup web UI property	No equivalent exists in the host properties.

Installing KMS

The following procedure describes how to install KMS.

Note: For more information about configuring KMS in a Cloud storage environment refer to the NetBackup Cloud Administrator's Guide.

The KMS service is called `nbkms`.

The service does not run until the data file has been set up, which minimizes the effect on environments not using KMS.

To install KMS

1. Run the `nbkms -createemptydb` command.
2. Enter a pass phrase for the host master key (HMK). You can also press **Enter** to create a randomly generated key.
3. Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.
4. Enter a pass phrase for the key protection key (KPK).

5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.

The KMS service starts when after you enter the ID and press Enter.

6 Start the KMS service as follows:

On UNIX, run the following command:

```
/usr/openv/netbackup/bin/nbkms
```

On Windows, do the following:

```
Start > Run > Services.msc > Start the NetBackup Key Management
Service
```

7 Use the `grep` command to ensure that the service has started, as follows: `ps -ef | grep nbkms`

8 Run the following command to register the `nbkms` service with NetBackup web services:

```
nbkmscmd -discovernbkms
```

9 Create the key group. The key group name must be an identical match to the volume pool name. All key group names must have a prefix `ENCR_`.

Note: When using key management with Cloud storage and PureDisk, the `ENCR_` prefix is not required for the key group name.

To create a (non-Cloud storage) key group use the following command syntax.
`nbkmsutil -createkg -kgname ENCR_`*`volumepoolname`*

The `ENCR_` prefix is essential. When BPTM receives a volume pool request that includes the `ENCR_` prefix, it provides that volume pool name to KMS. KMS identifies it as an exact match of the volume pool and then picks the active key record for backups out of that group.

To create a Cloud storage key group use the following command syntax.

```
nbkmsutil -createkg -kgname storage_server_name:volume_name
```

10 Create a key record by using the `-createkey` option.

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname
-activate -desc "message"
```

The key name and message are optional; they can help you identify this key when you display the key.

The `-activate` option skips the prelive state and creates this key as active.

11 Provide the pass phrase again when the script prompts you.

In the following example the key group is called `ENCR_pool1` and the key name is `Q1_2008_key`. The description explains that this key is for the months January, February, and March.

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key
-activate -desc "key for Jan, Feb, & Mar"
```

12 You can create another key record using the same command; a different key name and description help you distinguish they key records: `nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for Apr, May, & Jun"`

Note: If you create more than one key record by using the command `nbkmsutil -kgname` *`name`* `-activate`, only the last key remains active.

---

13 To list all of the keys that belong to a key group name, use the following command:

`nbkmsutil -listkeys -kgname` *keyname*

Note: You need the passphrase, salt (if applicable), key group name, and key tag to recover this key if it is lost. You must store all this information at a secure place. Salt, key group name, and key tag can be found in the output of the `nbkmsutil -listkeys` command execution.

The following command and output use the examples in this procedure.

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name        : ENCR_pool1
Supported Cipher      : AES_256
Number of Keys        : 2
Has Active Key        : Yes
Creation Time         : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description           : -
 Key Tag    : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
 Key Name              : Q2_2013_key
 Current State         : ACTIVE
 Creation Time         : Thu Aug  8 16:25:19 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Apr, May, & Jun
 FIPS Approved Key     : No

 Key Tag    : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
 Key Name              : Q1_2013_key
 Current State         : INACTIVE
 Creation Time         : Thu Aug  8 16:25:03 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Jan, Feb, & March
 FIPS Approved Key     : No
Number of Keys: 2
```

Workflow for external KMS configuration

For external KMS integration, centralized configuration on the NetBackup primary server is used. The primary server should establish an outbound connection with the KMIP port on the external KMS server. Configure the communication channel with external KMS on the primary server with certificate credentials. The primary server then sends all the requests to the external KMS servers on behalf of other servers such as media servers.

Table 4-8 Workflow to configure a KMS

Step number	Step	Reference topic
Step 1	Validate KMS credentials	See "Validating KMS credentials" on page 132.
Step 2	Configure KMS credentials	See "Configuring KMS credentials" on page 133.
Step 3	Configure KMS	See "Configuring KMS" on page 135.
Step 4	Create keys	See "Creating keys in an external KMS" on page 135.
Step 5	Configure storage	Refer to the NetBackup Administrator's Guide, Volume I.
Step 6	Configure policy	Refer to the NetBackup Administrator's Guide, Volume I.

Validating KMS credentials

If incorrect credentials are configured in NetBackup, communication with external KMS server may fail. To avoid such failures, you can carry out certain validations before a credential can be configured for the KMS use. If a validation check is not passed, the credential cannot be configured.

See "Configuring KMS credentials" on page 133.

The `-validate` command option is useful when the KMS vendor is listed as a supported KMS vendor in the NetBackup hardware compatibility list.

The following validations are carried out while you configure a new credential or update an existing one.

It is not recommended to configure credentials if one or more checks fail:

- The certificate path is valid

- The truststore path is valid
- The private key path is valid
- The certificates in certificate chain are readable
- The certificates in a truststore are readable
- The private key is readable
- The Common Name field is not empty
- The certificate is not expired
- The certificate is currently valid
- The private key matches the certificate
- The certificates are in the appropriate order
- The following CRL validation checks are performed, if the `ECA_CRL_PATH` is configured and the CRL check level is other than DISABLE:
  - The CRL directory consists of CRL files
  - The CRL check level is valid
  - The CRL path is valid
  - The available CRLs are readable

To validate KMS credentials and KMS functionality

1. Run the following command:

   ```
   nbkmiputil -validate -kmsServer kms_server_name -port port
   -certPath cert_path -privateKeyPath private_key_path
   -trustStorePath trust_store_path
   ```

   The `nbkmiputil` command validates the KMS functionality including connection to the KMS server.

   It also tests operations like list keys, fetch keys, set attributes, and fetch attributes. For set attributes, you must have the 'write' permission for the KMS server. The `nbkmiputil` command also validates CA fingerprint on the server certificate that is exchanged through TLS handshake. `nbkmiputil` uses TLS 1.2 or later protocol for secure communication with external KMS server.

2. If the check fails, contact Cohesity Technical Support.

Configuring KMS credentials

To configure external KMS in NetBackup, you need to first configure the credentials that NetBackup uses to authenticate with the external KMS server. As part of this

step, you need to specify the path for public key Infrastructure (PKI) artifacts that are required for certificate-based authentication. The following information is required:

- Certificate file path
- Keystore file path
- Trust store file path
- Passphrase or passphrase file path

Note: After external KMS configuration or keys are updated, NetBackup may take several minutes to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 minutes (for external KMS). To immediately consume a key, cache can be cleared by executing the following command on the respective media server:

```
bpclntcmd -clear_host_cache
```

To configure KMS credentials

- Run the `nbkmscmd -configureCredential` command:

  This command creates a copy of files that are provided on the command-line interface and stores them into the credentials database. When the command is successfully executed, you can delete these files if you do not need them. NetBackup does not track any updates to these files. If the certificate needs to be updated, typically in case of renewal, you need to run the `nbkmscmd -updateCredential` command again with new certificate files.

  ```
  nbkmscmd -configureCredential -credName credential_name -certPath
  certificate_file_path -privateKeyPath private_key_file_path
  -trustStorePath CA_certificate_file_path [-passphrasePath
  private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN |
  DISABLE] [-server master_server_name] [-description description]
  ```

Configuring KMS

To configure NetBackup KMS (NBKMS)

- Run the following command:

  ```
  nbkmscmd -configureKMS -name configuration_name -type NBKMS -hmkId
  host_master_key_ID_to_identify_HMK_passphrase -kpkId
  key_protection_key_ID_to_identify_KPK_passphrase
  [-useRandomPassphrase 0 | 1] [-enabledForBackup 0 | 1] [-priority
  priority_of_KMS_server] [-server master_server_name] [-description
  description]
  ```

To configure external KMS

- Run the following command:

  ```
  nbkmscmd -configureKMS -name configuration_name -type KMIP -port
  port_to_connect_to_external_KMS_server -kmsServerName
  network_name_of_external_KMS_server -credId credential_ID |
  -credName credential_name [-enabledForBackup 0 | 1] [-priority
  priority_of_KMS_server] [-server master_server_name] [-description
  description]
  ```

Creating keys in an external KMS

You can use NetBackup to create keys in an external KMS. NetBackup must have the required permissions to create keys in the external KMS.

To create keys in an external KMS

- Run the following command:

  ```
  nbkmscmd -createkey -name configuration_name -keyGroupName
  keygroup_name -keyName key_name -comment comments
  ```

  The `createKey` command creates a key in active state. For external KMS, you can have multiple active keys in a key group. NetBackup uses the latest active key. The command also sets all the required attributes for the key.

Note: After any update in external KMS configuration or key related changes, NetBackup may take some time to consume appropriate key in backup or restore workflow. This is because NetBackup caches the key for 10 min (for external KMS). To consume the key immediately, run the following command on the respective media server to clear the cache:

```
bpclntcmd -clear_host_cache.
```

Workflow to configure data-in-transit encryption

This topic provides the steps to carry out data-in-transit encryption (DTE) in your NetBackup environment. The DTE configuration comprises the following two primary options:

- Global DTE mode
- Client DTE mode

Table 4-9 Workflow of DTE configuration

Step number	Step	Reference topic
Step 1	Review the configuration settings of the global DTE mode option and configure the option as per your DTE requirements	See "Configure the global data-in-transit encryption setting" on page 136.
Step 2	Review the configuration settings of the client DTE mode option and configure the option as per your DTE requirements	See "Configure the DTE mode on a client" on page 137.
Step 3	Review how the decision about data encryption is made based on the NetBackup operation that you want to perform and the DTE configuration settings.	See "How DTE configuration settings work in various NetBackup operations" on page 139. **Note:** If you plan to modify any existing DTE configuration settings, you must review this topic to understand the impact on the NetBackup operations.

Apart from the primary DTE configuration settings, the following settings are used in certain scenarios:

- Media server DTE mode
  See "Configure the DTE mode on the media server" on page 159.
- Backup image DTE mode
  See "Modify the DTE mode on a backup image" on page 159.
  See "DTE_IGNORE_IMAGE_MODE for NetBackup servers" on page 160.

Configure the global data-in-transit encryption setting

To configure the data-in-transit encryption (DTE) in your NetBackup environment, you need to first set the global DTE configuration setting (or global DTE mode) and then the client DTE mode.

Data-in-transit encryption decision for various NetBackup operations is carried out based on the global DTE mode, the client DTE mode, and the image DTE mode.

The supported values for the global DTE mode are as follows:

- `Preferred Off`: Specifies that the data-in-transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.
- `Preferred On`: Specifies that the data-in-transit encryption is enabled only for NetBackup 9.1 and later clients.
  In case of fresh NetBackup installation, the global DTE mode is set to `Preferred On` by default.
  In case of NetBackup upgrade, the previous setting is retained.
  This setting can be overridden by the NetBackup client setting.
- `Enforced`: Specifies that the data-in-transit encryption is enforced if the NetBackup client setting is either 'Automatic' or 'On'. With this option selected, jobs fail for the NetBackup clients that have the data-in-transit encryption set to 'Off' and for the hosts earlier than 9.1.

Note: By default, the DTE mode for 9.1 clients is set to `Off` and for 10.0 and later clients, it is set to `Automatic`.

See "DTE_CLIENT_MODE for clients" on page 138.

RESTful API to be used for the global DTE configuration:

- GET - /security/properties
- POST - /security/properties

To set or view the global DTE mode using the NetBackup web UI

1. At the top right, select **Security > Global security**.
2. On the **Secure communication** tab, select one of the following global DTE settings:
   - `Preferred Off`
   - `Preferred On`
   - `Enforced`

Configure the DTE mode on a client

The `DTE_CLIENT_MODE` configuration option specifies the data-in-transit encryption (DTE) mode that is set on the NetBackup client.

See "DTE_CLIENT_MODE for clients" on page 138.

You can update and view the client DTE mode using the following commands:

`bpsetconfig`/`nbsetconfig` and `bpgetconfig`/`nbgetconfig`

DTE_CLIENT_MODE for clients

The `DTE_CLIENT_MODE` option specifies the data-in-transit encryption (DTE) mode that is set on the NetBackup client.

Table 4-10 DTE_CLIENT_MODE information

Usage	Description
Where to use	On NetBackup clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `DTE_CLIENT_MODE = AUTOMATIC | ON | OFF` By default, the DTE mode for 9.1 clients is set to `OFF` and for 10.0 and later clients, it is set to `AUTOMATIC`. ■ If the `DTE_CLIENT_MODE` option is set to `AUTOMATIC`, the client follows the DTE mode that is set at the global level: `Enforced`, `Preferred On`, or `Preferred Off`. ■ If the option is set to `ON`, data-in-transit encryption is enabled for the client. ■ If the option is set to `OFF`, data-in-transit encryption is disabled for the client. This setting can be used to exclude a client for encryption if the global DTE mode is set to `Preferred On`. **Note:** If the global DTE mode is set to `Enforced`, jobs fail for the NetBackup clients that have the `DTE_CLIENT_MODE` option set to 'OFF' and also for the hosts earlier than 9.1.
Equivalent NetBackup web UI property	No equivalent exists. Global settings are configured in **Settings > Global security > Secure communication > Data-in-transit encryption**.

How DTE configuration settings work in various NetBackup operations

This topic provides information on how you can change the DTE configuration settings to achieve the required data-in-transit encryption with respect to various NetBackup operations.

Review the following reference topics before you modify any DTE configuration settings.

The following tables show how DTE setting (unencrypted or encrypted) is decided for a certain NetBackup workflow under different NetBackup configurations along with DTE configuration settings.

Backup

In the backup workflow, data is transferred between a media server and a client as part of a backup job.

Figure 4-1 Backup workflow

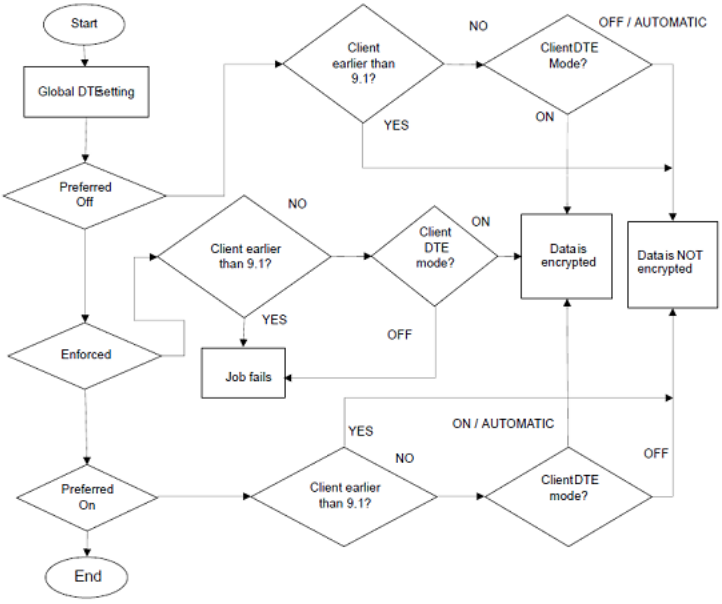


Table 4-11 The media server DTE mode is On (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted	Operation fails

Table 4-12 The media server DTE mode is Off (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails	Operation fails

Restore

In the restore workflow, there can be two DTE scenarios:

- When the image DTE mode is Off
- When the image DTE mode is On

In either of the scenarios, there can be one or more media servers involved (if multiple images are selected) while restoring data on a client for single NetBackup job.

Image DTE mode is Off

Table 4-13 Media server DTE mode is On (default)

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted	Data is not encrypted

Table 4-13 Media server DTE mode is On (default) *(continued)*

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted	Operation fails

Table 4-14 Media server DTE mode is Off

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Operation fails	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails	Operation fails

Table 4-15 Mixed media servers (9.1 and 10.0 or later) - Media1: DTE mode On, Media2: DTE mode Off

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Preferred Off	Media1 - Data is encrypted Media2 - Operation fails Job state - Partial Success Job DTE mode - On	Media1- Data is not encrypted Media2 - Data is not encrypted	Media1- Data is not encrypted Media2 - Data is not encrypted	Media1- Data is not encrypted Media2 - Data is not encrypted
Preferred On	Media1- Data is encrypted Media2- Operation fails Job state - Partial Success Job DTE mode - On	Media1- Data is not encrypted Media2 - Data is not encrypted	Media1 - Data is encrypted Media2 - Data is not encrypted Job DTE mode - Off	Media1- Data is not encrypted Media2 - Data is not encrypted

Table 4-15 Mixed media servers (9.1 and 10.0 or later) - Media1: DTE mode On, Media2: DTE mode Off *(continued)*

Global DTE mode	DTE mode of NetBackup client 9.1 or later			NetBackup host (media server or client) earlier than 9.1
	On	Off	Automatic	
Enforced	Media1 - Data is encrypted Media2 - Operation fails Job state - Partial Success Job DTE mode - On	Media1 - Operation fails Media2 - Operation fails Job state - Fail	Media1 - Data is encrypted Media2 - Operation fails Job state - Partial Success Job DTE mode - On	Media1 - Operation fails Media2 - Operation fails Job state - Operation fails

Image DTE mode is On

If the image DTE mode is On, the default behavior is to restore with data-in-transit encryption for 9.1 and later hosts and to fail the job if any DTE unsupported host involves in the workflow . However, you can still restore by ignoring the image DTE mode.

Use the `DTE_IGNORE_IMAGE_MODE` configuration option that is to be set on the primary server. Possible values: `NEVER` (default) | `ALWAYS` | `WHERE_UNSUPPORTED`

Table 4-16 When the image DTE mode is On and the media server DTE mode is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted

Table 4-16 When the image DTE mode is On and the media server DTE mode is On *(continued)*

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred On	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	NetBackup client 9.1 or later with DTE mode ON	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Operation fails
	NetBackup client 9.1 or later with DTE mode AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Operation fails	Operation fails

Table 4-17 When the image DTE mode is On and the DTE setting on 10.0 and later media server is Off

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Data is not encrypted
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Data is not encrypted
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	NetBackup Client 9.1 or later with DTE mode ON	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode OFF	Operation fails	Operation fails	Operation fails
	NetBackup Client 9.1 or later with DTE mode AUTOMATIC	Operation fails	Operation fails	Operation fails
	NetBackup host earlier than 9.1 (either media server or client)	Operation fails	Operation fails	Operation fails

Note: If the `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-14.

MSDP backup, restore, and optimized duplication

Data-in-transit encryption (DTE) feature is now integrated with MSDP storage server for backup and restore workflows.

For backup on MSDP disk pool, the encryption of data path from client to media server is controlled by the NetBackup DTE settings (global and client DTE modes).

If the MSDP storage server has multiple load balancing media servers attached to it and if the selected media server is 10.0.0.1 or later, the storage server must be 10.0.0.1 or later. Else, backup job fails. You must upgrade the 10.0 storage server to 10.0.0.1. If the load balancing media server is 10.0 or earlier, the data may be transferred in plain text and job is always successful, even if DTE was to be honored.

Ideally, you must have load balancing media servers and storage servers with 10.0.0.1 or later when DTE is enabled.

These given conditions are also valid for the optimized duplication workflow.

In case of mixed environment, where either storage server or one of the load balancing media servers is earlier than 10.0, the following configuration will be required in order to honor an end-to-end encryption:

- DTE should be enabled from NetBackup side based on DTE configurations i.e. Global/Media Server/Client Settings
- Encryption should be enabled from MSDP side using ENCRYPTION flag in pd.conf
  See the *NetBackup Deduplication Guide* for details on enabling the encryption using MSDP.

Note: If data-in-transit encryption is enabled in NetBackup and the `ENCRYPTION` flag in `pd.conf` is also enabled, MSDP encryption takes the precedence over NetBackup DTE. It results into data-at-rest encryption and not in data-in-transit encryption.

Universal-Share policy backup

For Universal-Share policy type, client selection can either be storage server name where the Universal Share resides or the host name where the Universal Share is mounted. So the client for this policy type can be a host where the NetBackup client software is not installed.

Because of this limitation, NetBackup cannot check the client DTE mode. It checks for the global and media server DTE modes for Universal-Share policy backup and works as per the following table:

Table 4-18 DTE for Universal-Share policy backup

Global DTE mode	DTE mode of media server 9.1 or later		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Catalog backup and recovery

Media server should be of the same NetBackup version as the primary server for catalog backup and recovery workflow.

Review the following points:

- DTE mode for catalog backup jobs is similar to the file system workflow and DTE decision is similar to the backup workflow described above.
- DTE mode in catalog backup jobs:
  - Parent catalog backup job does not have DTE mode set.
  - Database staging child job does not have DTE mode set.
  - Other child jobs have DTE mode set as per the configured DTE settings.
- DTE mode in catalog recovery jobs:
  - First 2 jobs have the DTE mode set as per the following tables depending on the image DTE mode.
  - The first two jobs replace the global DTE setting and primary server's bp.conf values, so the 3rd job DTE mode is set as per the recovered global DTE setting and primary server's bp.conf values.

The image DTE mode is Off

Table 4-19 When the image DTE mode is Off and the media server DTE setting is On

Global DTE mode	NetBackup Primary server 9.1 and later with DTE mode		
	On	**Off**	**Automatic**
Preferred Off	Data is encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted
Enforced	Data is encrypted	Data is encrypted	Data is encrypted

Note: When the global DTE setting is set to `ENFORCED` and the `DTE_CLIENT_MODE` is Off, DTE is preferred over failure in case of catalog recovery.

Table 4-20 When the image DTE mode is Off and the media server DTE setting is Off

Global DTE mode	NetBackup Primary server 9.1 and later with DTE mode		
	On	**Off**	**Automatic**
Preferred Off	Data is encrypted *	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted *	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted *	Data is encrypted *	Data is encrypted *

* signifies that DTE is preferred over failure during catalog recovery. It ignores the DTE setting on the media server, that is Off unless the client DTE mode is set to Automatic.

The image DTE mode is On

Table 4-21 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is not encrypted
Preferred On	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted
Enforced	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted	Data is encrypted	Data is encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted	Data is encrypted	Data is encrypted

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-19.

Table 4-22 When the image DTE mode is On and the media server DTE setting is Off

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is not encrypted
Preferred On	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is not encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is not encrypted
Enforced	Primary server with DTE_CLIENT_MODE as ON	Data is encrypted *	Data is encrypted *	Data is encrypted *
	Primary server with DTE_CLIENT_MODE as OFF	Data is encrypted *	Data is encrypted *	Data is encrypted
	Primary server with DTE_CLIENT_MODE as AUTOMATIC	Data is encrypted *	Data is encrypted *	Data is encrypted *

* signifies that DTE is preferred over failure during catalog recovery. It ignores the DTE setting on the media server, that is Off unless the client DTE mode is set to Automatic.

Duplication

In the duplication workflow, a backup copy is copied from one storage unit to another storage unit, so there is no client that comes into picture. The hosts that participate are source media server and target media server from the same domain.

Table 4-23 The image DTE mode is Off

Global DTE mode	Both media servers are 9.1 or later with DTE mode		One of the media servers is earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-24 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Both NetBackup media servers 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	Both NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	Both NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-23.

Table 4-25 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER	**WHERE_UNSUPPORTED**	**ALWAYS**
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Synthetic backup

A synthetic backup can be a synthetic full or a synthetic cumulative backup. The images that are used to create the synthetic image are known as component images. For instance, the component images in a synthetic full backup are the previous full image and the subsequent incremental images. A typical NetBackup backup process accesses the client to create a backup. A synthetic backup is a backup image created without using the client. Instead, a synthetic backup process creates a full or a cumulative incremental image by using previously created backup images called component images. In the synthetic backup workflow, images are fetched from different source storage units, synthesized, and copied to a target storage unit.

The hosts that come into the picture are source media servers and target media server from the same domain.

Table 4-26 DTE mode is OFF in the image

Global DTE mode	All NetBackup media server 9.1 and later with DTE mode		Any NetBackup media server earlier than 9.1
	On	**Off**	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-27 When DTE mode is On for any one of the images and media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	All NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Any NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-26.

Table 4-28 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-26.

Note:

Verify

In the verification workflow, backup image header is read, and its integrity is checked with the catalog. Therefore, a client does not come into picture. The hosts that participate are media server and primary server from the same domain.

Table 4-29 The image DTE mode is Off

Global DTE mode	NetBackup media server 9.1 and later with DTE mode		NetBackup media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-30 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	DTE mode of NetBackup client 9.1 or later	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	Media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Preferred On	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Media server earlier than 9.1	Operation fails	Data is not encrypted	Data is not encrypted
Enforced	Media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	Media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Table 4-31 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Import

In the import workflow, backup image is read from the storage unit and the NetBackup catalog is created. Therefore, a client does not come into picture. The hosts that participate are the media server and the primary server from the same domain.

Note: If you want to retain the DTE controls based on the image, you must upgrade the media servers that are to be used for the import operations to NetBackup 10.0 before you perform the import operation.

The following table is applicable for all import workflows such as phase-1 import, phase-2 import and Storage Lifecycle Policy (SLP) import.

Table 4-32 DTE mode is OFF in the image

Global DTE mode	Media server 9.1 or later with DTE mode		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is not encrypted
Enforced	Data is encrypted	Operation fails	Operation fails

Table 4-33 When the image DTE mode is On and the media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup media server earlier than 9.1	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is not encrypted	Data is not encrypted	Data is not encrypted
Enforced	NetBackup media server 9.1 and later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Operation fails	Operation fails	Operation fails

Note: For phase-1 import, you need to set `DTE_IGNORE_IMAGE_MODE` on the media server to ignore the DTE mode of the image for 9.1 and later media servers.

For phase-1 import scenario, NetBackup media server earlier than 9.1 is not aware of the DTE mode in the image. If the image was created with the DTE mode set to On, for phase-1 import, the job does not fail for media servers with version earlier than 9.1 and the image DTE mode is set to Off in the catalog.

Note: When `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, DTE decision is as per Table 4-32.

Table 4-34 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted

Table 4-34 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off *(continued)*

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	**WHERE_UNSUPPORTED**	**ALWAYS**
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-32.

MSDP SLP import at target domain

In this case, the image is already replicated in the target disk pool and now the intention is to create a catalog out of that image through SLP import policy. As this operation happens in the target domain and no cross-domain operation happens, the target DTE global setting comes into the picture.

If the replicated image has the DTE mode On, then irrespective of other DTE configurations, the import operation is carried out with DTE mode On.

If the replicated image has the DTE mode Off, the DTE mode is derived based on the target domain global DTE setting and import is carried out based on the derived DTE mode.

Review the following MSDP limitations that need to be considered for this workflow:

- If the MSDP storage server has multiple load balancing media servers attached to it and if the selected media server is 10.0.0.1 or later, the storage server must be 10.0.0.1 or later. Else, backup job fails. You must upgrade the 10.0 storage server to 10.0.0.1.
  If the load balancing media server is 10.0 or earlier, the data may be transferred in plain text and job is always successful, even if DTE was to be honored.
  Ideally, you must have load balancing media servers and storage servers with 10.0.0.1 or later when DTE is enabled.
- In case of mixed environment, where either storage server or even one of the load balancing media servers is of version earlier than 10.0, the following configuration is required in order to honor end-to-end encryption:
  - DTE should be enabled from NetBackup side based on the DTE configuration settings - global / media server / client DTE mode
  - Encryption should be enabled from MSDP side using the `ENCRYPTION` flag in pd.conf

Refer to the NetBackup Deduplication Guide for details on enabling encryption using MSDP.

Note: If you set DTE On for NetBackup, but the ENCRYPTION flag in pd.conf is not enabled, the data path from the load balancing media server to the storage server is not encrypted. However, the job DTE mode and the image DTE mode may be On.

If DTE is enabled at the NetBackup side and encryption is enabled from MSDP side (`ENCRYPTION` flag in pd.conf), MSDP encryption takes the precedence over NetBackup DTE. It results in data-at-rest encryption and not data-in-transit encryption.

Replication

If the MSDP storage server is used for replication, the following considerations need to be reviewed:

- The Data-in-transit (DTE) encryption feature is not integrated with MSDP storage for replication workflows and it is controlled by the `OPTDUP_ENCRYPTION` flag in pd.conf.
- The job DTE mode depends on the image DTE mode or the global DTE setting of the source domain.
- The correct values must be set for the DTE configuration settings and the `OPTDUP_ENCRYPTION` flag for the source and target domains.

For details on enabling encryption using MSDP, see the *NetBackup Deduplication Guide*.

Table 4-35 The image DTE mode is Off

Global DTE mode	Media server 9.1 or later with DTE mode		Media server earlier than 9.1
	On	Off	
Preferred Off	Data is not encrypted	Data is not encrypted	Data is not encrypted
Preferred On	Data is encrypted	Data is not encrypted	Data is encrypted
Enforced	Data is encrypted	Operation fails	Data is encrypted

Table 4-36 When the image DTE mode is On and media server DTE setting is On

Global DTE mode	Host	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
		NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is not encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is not encrypted
Preferred On	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is encrypted
Enforced	NetBackup media server 9.1 or later	Data is encrypted	Data is encrypted	Data is encrypted
	NetBackup media server earlier than 9.1	Data is encrypted	Data is encrypted	Data is encrypted

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-35.

Table 4-37 When the image DTE mode is On and the media server DTE setting on 10.0 or later is Off

Global DTE mode	Value of the DTE_IGNORE_IMAGE_MODE configuration option		
	NEVER (default)	WHERE_UNSUPPORTED	ALWAYS
Preferred Off	Operation fails	Operation fails	Data is not encrypted
Preferred On	Operation fails	Operation fails	Data is not encrypted
Enforced	Operation fails	Operation fails	Operation fails

Note: If `DTE_IGNORE_IMAGE_MODE` is set to `ALWAYS`, the DTE decision is as per the table - Table 4-35.

Configure the DTE mode on the media server

The media server setting can be used only to turn off data-in-transit encryption (DTE) for NetBackup operations.

In a NetBackup configuration where a media server is slow because of the old hardware, you can turn off the media server DTE mode so that there is no performance issue. However, it is recommended that you upgrade the old media server hardware. This setting is available for media servers with NetBackup 10.0 and later.

RESTful API to be used for the global DTE configuration:

- GET - /config/media-servers/{hostName}
- PATCH - /config/media-servers/{hostName}

To set or view the media server DTE mode

1. Ensure that you have an RBAC role with the following permissions on the media server resource:
   - View
   - Update
   - Manage access
2. Run the following command to set the media server DTE mode:

   ```
   nbseccmd -setsecurityconfig -dtemediamode off|on -mediaserver
   media_server_name
   ```
3. Run the following command to view the media server DTE mode:

   ```
   nbseccmd -getsecurityconfig -dtemediamode -mediaserver
   media_server_name
   ```

   Note: For 9.1 media servers, you can only view the DTE mode as `On`, but you cannot set it.

Modify the DTE mode on a backup image

The data-in-transit (DTE) feature of NetBackup introduces an additional image attribute (DTE mode) when a backup image is created.

Primarily, the global DTE mode and the client DTE mode decide whether the data-in-transit encryption takes place or not for a NetBackup operation. If the data

is encrypted during backup, the DTE mode attribute of the associated NetBackup image is set to `On`.

If based on the global DTE mode and the client DTE mode, the data cannot be encrypted during backup, the DTE mode attribute of the image is set to `Off`.

The image DTE mode should be honored and retained for all subsequent operations on that image. For example, restore and secondary operations like duplication, replication, import and so on. If the image DTE mode is set to On, subsequent operations always encrypt the data for DTE supported hosts.

If the host does not support DTE, then the job fails. If the image DTE mode is set to Off, the DTE for subsequent operations is decided based on the global and client DTE modes at that point of time. This is the default behavior.

In certain cases, you may want to modify the image DTE mode that was set at the time of its creation.

RESTful API to be used to modify the image DTE mode:

- PATCH - /catalog/images/{backupId}

To modify the image DTE mode

- Run the following command:

  ```
  bpimage -update -image_dtemode Off|On
  ```

  You can also change the image DTE mode using the **NetBackup Web UI > Catalog** node.

See "DTE_IGNORE_IMAGE_MODE for NetBackup servers" on page 160.

DTE_IGNORE_IMAGE_MODE for NetBackup servers

Use the `DTE_IGNORE_IMAGE_MODE` option if you do not want the data to be encrypted even if the data-in-transit encryption (DTE) mode of the backup image is enabled.

The `DTE_IGNORE_IMAGE_MODE` option is applicable for all backup images.

Table 4-38 DTE_IGNORE_IMAGE_MODE information

Usage	Description
Where to use	On NetBackup servers.

Table 4-38 DTE_IGNORE_IMAGE_MODE information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `DTE_IGNORE_IMAGE_MODE = NEVER | ALWAYS | WHERE_UNSUPPORTED` The default value of the `DTE_IGNORE_IMAGE_MODE` option is `NEVER`. ■ `NEVER` - Use this option to specify that the data-in-transit encryption takes place based on the DTE mode of the image. ■ `ALWAYS` - Use this option to specify that the DTE mode of the image is always ignored during data-in-transit encryption irrespective of whether the NetBackup host supports the encryption or not. Data-in-transit encryption takes place based on the global DTE mode and client DTE mode. ■ `WHERE_UNSUPPORTED` - Use this option if you have NetBackup hosts earlier than 9.1 in your environment and you do not want the jobs to fail for these hosts when the DTE mode is enabled for the image. With this configuration, data-in-transit encryption happens based on the global and client DTE mode settings. The image DTE mode is ignored.
Equivalent NetBackup web UI property	No equivalent exists.

Workflow to use external certificates for NetBackup host communication

To configure NetBackup to use external CA-signed certificates for secure communication, you should carry out the following steps in the given order:

Table 4-39 Workflow to use external certificates for NetBackup host communication

Step	Description
Step 1	Ensure the following: ■ The external certificates for the web server, primary server, and all hosts are placed at the appropriate locations. ■ In case of file-based certificates, the private key files for the external certificates are placed at the appropriate locations. See "ECA_PRIVATE_KEY_PATH for NetBackup servers and clients" on page 181. If the private keys are encrypted, passphrase files should be placed at the appropriate locations. See "ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients" on page 182. ■ The CRLs are placed at the required locations on the hosts as per their CRL configuration options and they are accessible. See "About certificate revocation lists for external CA" on page 163.
Step 2	Install the NetBackup software on the primary server (or upgrade the primary server).
Step 3	Enable the NetBackup domain to use external certificates by configuring the NetBackup web server. See "Configure an external certificate for the NetBackup web server" on page 166.
Step 4	Configure an external certificate for the NetBackup primary server host. See "Configuring the primary server to use an external CA-signed certificate" on page 167.
Step 5	Install the NetBackup software on the media server and clients (or upgrade the media server and clients). If the primary server is configured to use external certificates, the Installer prompts you to provide external certificate information for the host.

Table 4-39 Workflow to use external certificates for NetBackup host communication *(continued)*

Step	Description
Step 6	**Note:** This step is required for the hosts (media server and clients) that have the current NetBackup software, but are not configured to use external certificate. NetBackup hosts may not have external certificate configuration because of the following reasons: ■ You did not provide the external certificate information during installation or upgrade of the host. ■ The NetBackup primary server was not configured to use external certificates during installation or upgrade of the host. Configure an external certificate for a NetBackup host (media server or client) after installation. See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 173.

About certificate revocation lists for external CA

Certificate revocation list (CRL) for an external certificate authority (CA) contains a list of digital certificates that the external CA has revoked before the scheduled expiration date and should no longer be trusted.

NetBackup supports PEM and DER formats for CRLs for external CA.

CRLs for all CRL issuers or external CAs are stored in the NetBackup CRL cache that resides on each host.

During secure communication, each NetBackup host verifies the revocation status of the peer host's external certificate with the CRL that is available in the NetBackup CRL cache, based on the `ECA_CRL_CHECK` configuration option.

See "ECA_CRL_CHECK for NetBackup servers and clients" on page 183.

The NetBackup CRL cache is updated with the required CRLs using one of the following CRL sources:

`ECA_CRL_PATH` configuration option
: A NetBackup configuration option (from `bp.conf` file on UNIX or Windows registry) that specifies the path where the CRL exists.

  See "ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients" on page 185.

  See "How CRLs from ECA_CRL_PATH are used" on page 164.

CRL distribution point (CDP)	If you have not specified `ECA_CRL_PATH`, NetBackup downloads the CRLs from the URLs that are specified in the peer host certificate's CDP and caches them in the NetBackup CRL cache. See "How CRLs from CDP URLs are used" on page 165. NetBackup supports downloading CRLs from HTTP and HTTPS URLs that are specified in CDP.

The NetBackup CRL cache contains only the latest copy of a CRL for each CA (including root and intermediate CAs).

The `bpclntcmd -crl_download` service updates the CRL cache during host communication in the following scenarios irrespective of the time interval set for the `ECA_CRL_PATH_SYNC_HOURS` or `ECA_CRL_REFRESH_HOURS` options:

- When CRLs in the CRL cache are expired
- If CRLs are available in the CRL source (`ECA_CRL_PATH` or CDP), but they are missing from the CRL cache

---

Note: Once the `bpclntcmd -crl_download` service updates the CRLs in the CRL cache, it does not download the CRLs for the same CA for the next 15 min even though a valid download scenario has occurred. If you want to update the CRL within 15 min, terminate the `bpclntcmd -crl_download` service.

How CRLs from ECA_CRL_PATH are used

Use this section if you want to use `ECA_CRL_PATH` as the CRL source for the NetBackup CRL cache.

To use CRLs from ECA_CRL_PATH

1. Ensure that the CRLs for external CAs are stored in a directory and the directory path is accessible by the host.

   If you have a Flex Appliance application instance, the files must be stored in the following directory on the instance: `/mnt/nbdata/hostcert/crl`

   You can specify the CRL details that are required for external CA configuration during NetBackup installation or upgrade on the host.

   Select one of the following certificate revocation list (CRL) options during installation or upgrade:

   - **Use the CRL defined in the certificate** - No additional information is required.

- **Use the CRL at the following path** - You are prompted to provide a path to the CRL.

  If you choose to use the **Do not use a CRL** option, peer host's certificate is not verified with the CRL during host communication.

For more information, refer to the NetBackup Installation Guide.

2 Specify the CRL directory path for the `ECA_CRL_PATH` configuration option.

3 Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from `ECA_CRL_PATH`.

By default, CRLs from the cache are updated every one hour. To change the time interval, set the `ECA_CRL_PATH_SYNC_HOURS` option to a different value.

To manually update the CRL cache with the `ECA_CRL_PATH` CRLs, run the `nbcertcmd -updateCRLCache` command.

To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

How CRLs from CDP URLs are used

Use this section if you want to use CRL Distribution Point (CDP) as the CRL source for the NetBackup CRL cache.

To use CRLs from CDP

1 Ensure that the `ECA_CRL_PATH` configuration option is not specified.

2 Ensure that the host can access the URLs that are specified in the peer host's CDP.

3 Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from CDP URLs.

By default, CRLs are downloaded from the CDP after every 24 hours and updated in the CRL cache. To change the time interval, set the `ECA_CRL_REFRESH_HOURS` configuration option to a different value.

To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

Configure an external certificate for the NetBackup web server

Note: Before enrolling the certificate for the primary server, ensure that you complete the prerequisite steps as described in the following topic.

See "Workflow to use external certificates for NetBackup host communication" on page 161.

By default, NetBackup uses the security certificates that the NetBackup CA has issued. If you have a certificate that an external CA has issued, you can configure the NetBackup web server to use it for secure communication.

Note: Windows certificate store is not supported as certificate source for the NetBackup web server.

The API that you can use to configure the external certificate for the NetBackup web server: `POST security/web-certificates/{certificate_id}`.

If external certificate for the web server is configured using the API, the configuration process is audited.

To configure an external certificate for the web server

1. Ensure that you have valid certificate, private key of the certificate, and trusted CA bundle.
2. Ensure that the NetBackup Web Management Console service is up and running.
3. Run the following command:

   `configureWebServerCerts -addExternalCert -webUI -certPath` *`certificate path`* `-privateKeyPath` *`private key path`* `-trustStorePath` *`CA bundle path`* `[-passphrasePath` *`passphrase file path`*`]`

   The `configureWebServerCerts` command does not support use of Windows certificate store paths.

   Refer to the NetBackup Commands Reference Guide for more details on the command-line options.

   - In a clustered setup, to avoid a failover run the following command on the active node:

     `install_path``/netbackup/bin/bpclusterutil -freeze`

   - If the FIPS mode is enabled on the primary server, you can use only the PEM-formatted files for the `configureWebServerCerts` command.

4 Restart the NetBackup Web Management Console service to reflect the changes.

On UNIX, run the following commands:

- *install_path*/netbackup/bin/nbwmc -terminate
- *install_path*/netbackup/bin/nbwmc start

On Windows, use the **Services** application in the **Windows Control Panel**.

Location of the commands:

Windows	*install_path*\NetBackup\wmc\bin\install\
UNIX	*install_path*/wmc/bin/install

- In a clustered setup, unfreeze the cluster using the following command on the active node:
  install_path/netbackup/bin/bpclusterutil -unfreeze

5 Restart the NetBackup Messaging Queue Broker (nbmqbroker) service as follows:

On Windows:

Go to the **Services** application in the **Windows Control Panel** and manually restart the NetBackup Messaging Queue Broker service.

On UNIX:

Run the following command:

```
nbmqbroker stop; nbmqbroker start
```

6 Verify that you can access the NetBackup web user interface using a browser, without a certificate warning message.

Configuring the primary server to use an external CA-signed certificate

A NetBackup host ID-based certificate is deployed on the primary server during installation or upgrade. You can configure the primary server to use an external CA-signed certificate after installation. It includes:

- Defining the external certificate configuration options
  See "Configuration options for external CA-signed certificates" on page 176.
- Enrolling the external certificate for the primary server host

The enrolled certificate is used for communication between the host and the primary server domain that is listed in the `SERVER` configuration option on the host.

See "Configuring an external certificate for a clustered primary server" on page 169.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configure an external certificate for the NetBackup web server" on page 166.
- External certificates for the NetBackup web server and the primary server must be issued by the same root certificate authority.
  If the two certificate authorities do not match, communication between the **NetBackup Administration Console** and the NetBackup Web Management Console service (`nbwmc` service) fails.
- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
  If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
  See "About certificate revocation lists for external CA" on page 163.
- When NetBackup primary server is configured to use the service user (non-privileged user on UNIX and Local Service on Windows) to start most of the daemons or services, you must ensure that the following ECA paths are accessible to the service user:
  - ECA_CERT_PATH
  - ECA_PRIVATE_KEY_PATH
  - ECA_TRUST_STORE_PATH
  - ECA_KEY_PASSPHRASEFILE (optional)
  - ECA_CRL_PATH (optional)

  To grant access to the service user, do the following:
  On Unix, use the `chmod` or the `chown` command.
  On Windows run the following command:
  install_path\NetBackup\bin\goodies\nbserviceusercmd.exe -addAcl *ECA path* -reason *reason*

To configure the primary server to use an external certificate

1. Update the NetBackup configuration file (`bp.conf` file on UNIX or Windows registry) on the primary server with the external certificate-specific parameters.
   See "Configuration options for external CA-signed certificates" on page 176.

For Windows certificate store	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) ■ ECA_DR_BKUP_WIN_CERT_STORE (optional)
For file-based certificates	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_PRIVATE_KEY_PATH ■ ECA_TRUST_STORE_PATH ■ ECA_KEY_PASSPHRASEFILE (optional) ■ ECA_CRL_CHECK (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) **Note:** If you have a Flex Appliance application instance, the certificate files must be stored in the following directories on the instance: ECA_CERT_PATH, ECA_PRIVATE_KEY PATH, and ECA_TRUST_STORE_PATH: `/mnt/nbdata/hostcert/` ECA_CRL_PATH: `/mnt/nbdata/hostcert/crl`

2 Run the following command on the primary server to enroll an external certificate with the primary server domain that is defined in the `SERVER` option:

```
nbcertcmd -enrollCertificate
```

For more details on the command, refer to the NetBackup Commands Reference Guide.

Configuring an external certificate for a clustered primary server

Use this section to configure an external CA-signed certificate for a clustered primary server. The enrolled certificate is used for host communication.

Requirements

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configure an external certificate for the NetBackup web server" on page 166.
- Ensure that external certificates for the NetBackup web server and the virtual name are issued by the same certificate authority.
  If the two certificate authorities do not match, communication between the **NetBackup Administration Console** and the NetBackup Web Management Console service (`nbwmc` service) fails.

To enroll an external certificate for a clustered primary server

1. Update the NetBackup configuration file that is present on the shared disk (`nbcl.conf`) with the external certificate configuration options.

   See "Configuration options for external CA-signed certificates for a virtual name" on page 171.

   Use the `nbsetconfig` command to configure the following options:

   - `CLUSTER_ECA_CERT_PATH`
   - `CLUSTER_ECA_TRUST_STORE_PATH`
   - `CLUSTER_ECA_PRIVATE_KEY_PATH`
   - `CLUSTER_ECA_KEY_PASSPHRASEFILE` (optional)

   You need to configure the certificate revocation list (CRL) configuration options for each node.

   See "About certificate revocation lists for external CA" on page 163.

2. Run the following command on the primary server:

   ```
   nbcertcmd -enrollCertificate -cluster
   ```

   The enrolled certificate is used for communication between the active node and the primary server domain that is listed in the `SERVER` configuration option on the host.

   For more details on the command, refer to the *NetBackup Commands Reference Guide*.

3. Configure an external certificate on each cluster node.

   See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 173.

Configuration options for external CA-signed certificates for a virtual name

To configure a clustered NetBackup primary server to use external CA-signed certificate for host communication, you must define certain configuration options in the `nbcl.conf` file.

CLUSTER_ECA_CERT_PATH for clustered primary server

The `CLUSTER_ECA_CERT_PATH` option is specific to clustered primary server. It specifies the path to the external CA-signed certificate of the virtual name.

Table 4-40 CLUSTER_ECA_CERT_PATH information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_CERT_PATH = Path to the certificate of the virtual identity`
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

CLUSTER_ECA_TRUST_STORE_PATH for clustered primary server

The `CLUSTER_ECA_TRUST_STORE_PATH` option is specific to clustered primary server. It specifies the path to the certificate bundle file that contains all trusted root CA certificates in PEM format.

Table 4-41 CLUSTER_ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On clustered primary server.

Table 4-41 CLUSTER_ECA_TRUST_STORE_PATH information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_TRUST_STORE_PATH = Path to the external CA certificate`
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

CLUSTER_ECA_PRIVATE_KEY_PATH for clustered primary server

The `CLUSTER_ECA_PRIVATE_KEY_PATH` option is specific to clustered primary server. It specifies the path to the private key for the external CA-signed certificate of the virtual name.

If the virtual name certificate's private key is encrypted, you should define the `CLUSTER_ECA_KEY_PASSPHRASEFILE` option.

See "CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered primary server" on page 173.

Table 4-42 CLUSTER_ECA_PRIVATE_KEY_PATH information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `CLUSTER_ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate`
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered primary server

The CLUSTER_ECA_KEY_PASSPHRASEFILE option is specific to clustered primary server. It specifies the path to the text file where the passphrase for the virtual name certificate's private key is stored.

CLUSTER_ECA_KEY_PASSPHRASEFILE is optional. You should define this option if the virtual name certificate's private key is encrypted.

See "CLUSTER_ECA_PRIVATE_KEY_PATH for clustered primary server" on page 172.

Table 4-43 CLUSTER_ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On clustered primary server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: CLUSTER_ECA_KEY_PASSPHRASE_FILE = *Path to the passphrase file*
Equivalent NetBackup web UI property	No equivalent exists in the host properties.

Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation

A NetBackup host (media server or client) is configured to use an external certificate during installation or upgrade. You may choose to do the configuration after installation.

Use this section to configure a host to use an external certificate.

You can use this section to configure an external certificate for a cluster node.

The configuration steps include:

- Defining the external certificate configuration options
  See "Configuration options for external CA-signed certificates" on page 176.
- Ensuring that automatic enrollment is enabled - ECA_DISABLE_AUTO_ENROLLMENT is set to TRUE - or enrolling the external certificate manually for the host
  See "Enrolling an external certificate for a remote host" on page 175.

The enrolled certificate is used for communication between the host and the primary server domain that is listed in the `SERVER` configuration option on the host.

The enrolled certificate is used for host communication.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configure an external certificate for the NetBackup web server" on page 166.
- It is recommended that you enroll an external certificate for the primary server host before you enroll one for other hosts.
  See "Configuring the primary server to use an external CA-signed certificate" on page 167.
- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
  If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
  See "About certificate revocation lists for external CA" on page 163.

To configure a host (media server or client) to use an external certificate

1. Update the configuration file (`bp.conf` file or Windows registry) with the required external certificate-specific parameters on the host:

   See "Configuration options for external CA-signed certificates" on page 176.

For Windows certificate store	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) ■ ECA_DR_BKUP_WIN_CERT_STORE (optional)

For file-based certificates	Use the `nbsetconfig` command to configure the following parameters: ■ ECA_CERT_PATH ■ ECA_PRIVATE_KEY_PATH ■ ECA_TRUST_STORE_PATH ■ ECA_KEY_PASSPHRASEFILE (optional) ■ ECA_CRL_CHECK_LEVEL (optional) ■ ECA_CRL_PATH (optional) ■ ECA_CRL_PATH_SYNC_HOURS (optional) ■ ECA_CRL_REFRESH_HOURS (optional) **Note:** If you have a Flex Appliance application instance, the certificate files must be stored in the following directories on the instance: ECA_CERT_PATH, ECA_PRIVATE_KEY PATH, and ECA_TRUST_STORE_PATH: `/mnt/nbdata/hostcert/` ECA_CRL_PATH: `/mnt/nbdata/hostcert/crl`

2 Ensure that the `ECA_DISABLE_AUTO_ENROLLMENT` option is set to `TRUE` using the `nbgetconfig` command. This ensures that automatic enrollment is enabled.

If the option is disabled and you want to manually enroll the certificate, run the following command on the host to enroll an external certificate with the primary server domain that is defined in the `SERVER` configuration option on the host:

```
nbcertcmd -enrollCertificate
```

For more details on the command, refer to the *NetBackup Commands Reference Guide*.

Enrolling an external certificate for a remote host

Use this section to enroll an external certificate for a NetBackup host remotely. This lets the security administrator to enroll external certificate for multiple remote hosts from the same host.

To enroll an external certificate for a remote host (or to perform an enrollment sync operation on a remote host), ensure that the server from which you want to enroll the certificate is listed in the `SERVER` configuration option on the remote host.

To enroll certificate for a remote host

◆ Run the following command on the local host:

```
nbcertcmd -enrollCertificate -remoteHost remote_host_name -server
primary_server_name
```

An external certificate is enrolled for the specified remote host with the primary server that you provide with the `-server` option. This primary server must be available in the remote host's `SERVER` configuration option.

See "Configuration options for external CA-signed certificates" on page 176.

For more details on the commands, refer to the *NetBackup Commands Reference Guide*.

Configuration options for external CA-signed certificates

To configure a NetBackup primary server, media server, or client to use external CA-signed certificate for host communication, you must define certain configuration options in the NetBackup configuration file (`bp.conf` on UNIX platform or Windows registry).

About the mandatory and optional configuration options

- For external certificate configuration, for file-based certificates, the following configuration options are mandatory:
  - `ECA_CERT_PATH`
  - `ECA_TRUST_STORE_PATH`
  - `ECA_PRIVATE_KEY_PATH`
    If the private key of the external certificate is encrypted, `ECA_KEY_PASSPHRASEFILE` is also mandatory:
- For Windows certificate store, the following configuration options are mandatory:
  - `ECA_CERT_PATH`
- The following options are optional:
  - `ECA_CRL_CHECK`
    If the option is set to `DISABLE` (or `0`) the `ECA_CRL_PATH` option is ignored and revocation status of a peer host's certificate is not verified.
    If the option is set to a value other than `DISABLE` and `0`, revocation status of a peer host's certificate is verified based on `ECA_CRL_PATH`.
  - `ECA_DR_BKUP_WIN_CERT_STORE`
    For Windows certificate store, specify this option if you want to backup the external certificates during catalog backup.
  - `ECA_CRL_PATH_SYNC_HOURS`
    This option is used when `ECA_CRL_CHECK` is enabled and `ECA_CRL_PATH` is defined.

- ECA_CRL_REFRESH_HOURS

  This option is used when ECA_CRL_CHECK is enabled, but ECA_CRL_PATH is not defined (when CDP is used as a CRL source).

See "About certificate revocation lists for external CA" on page 163.

ECA_CERT_PATH for NetBackup servers and clients

The ECA_CERT_PATH option specifies the path to the external CA-signed certificate of the host. This option is mandatory.

NetBackup supports the following certificate sources for host certificates:

- Windows certificate store

  Note: The Windows certificate store is not supported for clustered primary servers.

- File-based certificates

Certificate order in the certificate file

A certificate file must have a certificate chain with certificates in the correct order. The chain starts with the server certificate (also known as the leaf certificate) and is followed by zero or more intermediate certificates. The chain must contain all intermediate certificates up to the Root CA certificate but should not contain the Root CA certificate itself. The chain is created such that each certificate in the chain signs the previous certificate in the chain.

The certificate file should be in one of the following formats:

- PKCS #7 or P7B file that is either DER or PEM encoded that has certificates in the specified order
- A file with the PEM certificates that are concatenated together in the specified order

Table 4-44 ECA_CERT_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-44 ECA_CERT_PATH information *(continued)*

Usage	Description

How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	For file-based certificates, use the following format:
	`ECA_CERT_PATH = Path to the external certificate of the host`
	For example: `c:\server.pem`
	If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
	For Windows certificate store, use the following format:
	`ECA_CERT_PATH = Certificate store name\Issuer name\Subject name`
	You can specify multiple certificate selection queries in a comma-separated format.
	`ECA_CERT_PATH = Store name1\Issuer name1\Subject name1,Store name2\Issuer name2\Subject name2`
	See "Specifying Windows certificate store for ECA_CERT_PATH" on page 178.

Equivalent NetBackup web UI property	No equivalent exists.

Specifying Windows certificate store for ECA_CERT_PATH

NetBackup selects a certificate from any of the local machine certificate stores on a Windows host.

In case of Windows certificate store, `ECA_CERT_PATH` is a list of comma-separated clauses.

Each clause is of the form *Store name**Issuer**Subject*. Each clause element contains a query.

`$hostname` is a keyword that is replaced with the fully qualified domain name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\"NetBackup\$hostname"`.

`$shorthostname` is a keyword that is replaced with the short name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\"NetBackup\$shorthostname"`.

The 'Store name' should be the exact name of the store where the certificate resides. For example: 'MY'

The 'Issuer' is optional. If this is provided, NetBackup picks the certificates for which the Issuer DN contains the provided substring.

The 'Subject' is mandatory. NetBackup picks the certificate for which the Subject DN contains the provided substring.

You must ensure to:

- Add the root certificate to Trusted Root Certification Authorities or Third-Party Root Certification Authorities in the Windows certificate store.
- If you have any intermediate CAs, add their certificates to the Intermediate Certification Authorities in the Windows certificate store.

Example - Certificate locations with WHERE CLAUSE:

- `My\Veritas\$hostname, My\ExampleCompany\$hostname`
  Where (certificate store is MY, Issuer DN contains `Veritas`, Subject DN contains `$hostname`) OR (certificate store name is `MY`, Issuer DN contains `ExampleCompany`, Subject DN contains `$hostname`)
- `MY\Veritas\"NetBackup\$hostname"`
  Where certificate store name is `MY`, Issuer DN contains `Veritas`, Subject DN contains `NetBackup\$hostname`
- `MY\\$hostname`
  Where certificate store name is `MY`, any Issuer DN, Subject DN contains `$hostname`
- `MY\\$shorthostname`
  Where certificate store name is `MY`, any Issuer DN, Subject DN contains `$shorthostname`
- `MY\Veritas\NetBackup $hostname`
  Where certificate store name is `MY`, Issuer DN contains `Veritas`, Subject DN contains `NetBackup $hostname`

If you provide a space between words, it is considered as a valid character.

Example - Certificate locations with invalid data:

- `MY\\`
  The Subject DN should have some value.

- `My\$hostname`

  The Subject DN should have some value.

- `\\$hostname`

  The certificate store name should have exact value of the store in which the certificate resides.

- `MY\CN=Veritas\CN=$hostname`

  The Subject DN and issuer DN cannot contain =, and also specific tags like CN=.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The `ECA_TRUST_STORE_PATH` option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

Do not specify the `ECA_TRUST_STORE_PATH` option if you use the Windows certificate store.

The trust store supports certificates in the following formats:

- PKCS #7 or P7B file having certificates of the trusted root certificate authorities that are bundled together. This file may either be PEM or DER encoded.
- A file containing the PEM encoded certificates of the trusted root certificate authorities that are concatenated together.

This option is mandatory for file-based certificates.

The root CA certificate in Cloudera distribution can be obtained from the Cloudera administrator. It may have a manual TLS configuration or an Auto-TLS enabled for the Hadoop cluster. For both cases, NetBackup needs a root CA certificate from the administrator.

The root CA certificate from the Hadoop cluster can validate the certificates for all nodes and allow NetBackup to run the backup and restore process in case of the secure (SSL) cluster. This root CA certificate is a bundle of certificates that has been issued to all such nodes.

Certificate from root CA must be configured under `ECA_TRUST_STORE_PATH` in case of self-signed, third party CA or Local/Intermediate CA environments. For example: In case of AUTO-TLS enabled Cloudera environments, you can typically find the root CA file named with `cm-auto-global_cacerts.pem` at path `/var/lib/cloudera-scm-agent/agent-cert`. For more details, refer Cloudera documentation.

Table 4-45 ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, or Nutanix AHV, this option must be set on the NetBackup primary server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_TRUST_STORE_PATH = Path to the external CA certificate` For example: `c:\rootCA.pem` If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
Equivalent UI property	No equivalent exists.

ECA_PRIVATE_KEY_PATH for NetBackup servers and clients

The `ECA_PRIVATE_KEY_PATH` option specifies the file path to the private key for the external CA-signed certificate of the host.

This option is mandatory for file-based certificates.

If the private key of the certificate is encrypted, you should specify the `ECA_KEY_PASSPHRASEFILE` option.

See "ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients" on page 182.

NetBackup supports PKCS #1 and PKCS #8 formatted private keys that are either plain text or encrypted. These may either be PEM or DER encoded. However, if it is PKCS #1 encrypted, it must be PEM encoded.

For encrypted private keys, NetBackup supports the following encryption algorithms:

- DES, 3DES, and AES if the private key is in the PKCS #1 format
- DES, 3DES, AES, RC2, and RC4 if the private key is in the PKCS #8 format

Note: You should not specify the `ECA_PRIVATE_KEY_PATH` option if Windows certificate store is specified for the `ECA_CERT_PATH` option.

See "ECA_CERT_PATH for NetBackup servers and clients" on page 177.

Table 4-46 ECA_PRIVATE_KEY_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate` For example: `c:\key.pem` If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/`.
Equivalent UI property	No equivalent exists.

ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients

The `ECA_KEY_PASSPHRASEFILE` option specifies the path to the text file where the passphrase for the external certificate's private key is stored.

You should specify the `ECA_KEY_PASSPHRASEFILE` option only if the certificate's private key is encrypted.

See "ECA_PRIVATE_KEY_PATH for NetBackup servers and clients" on page 181.

Note: You should not specify the `ECA_KEY_PASSPHRASEFILE` option if you use Windows certificate store.

See "ECA_CERT_PATH for NetBackup servers and clients" on page 177.

Note: Do not use the ECA_KEY_PASSPHRASEFILE on the MSDP servers that are used for MSDP direct cloud tiering as it is not supported with MSDP direct cloud tiering.

Table 4-47 ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_KEY_PASSPHRASEFILE = Path to the passphrase file`
Equivalent UI property	No equivalent exists.

ECA_CRL_CHECK for NetBackup servers and clients

The `ECA_CRL_CHECK` option lets you specify the revocation check level for external certificates of the host. It also lets you disable the revocation check for the external certificates. Based on the check, revocation status of the certificate is validated against the Certificate Revocation List (CRL) during host communication.

You can choose to use the CRLs from the directory that is specified for the `ECA_CRL_PATH` configuration option in the configuration file (`bp.conf` on UNIX or Windows registry) or the CRL Distribution Point (CDP).

See "ECA_CRL_PATH for NetBackup servers and clients" on page 184.

Table 4-48 ECA_CRL_CHECK information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-48 ECA_CRL_CHECK information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `HADOOP_CRL_CHECK = CRL check` You can specify one of the following: ■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. This is the default value. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent web UI property	No equivalent exists.

ECA_CRL_PATH for NetBackup servers and clients

The `ECA_CRL_PATH` option specifies the path to the directory where the Certificate Revocation Lists (CRL) of the external certificate authority (ECA) are located.

These CRLs are copied to NetBackup CRL cache. Revocation status of the external certificate is validated against the CRLs from the CRL cache.

CRL in the CRL cache is periodically updated with the CRL on the location that is specified for `ECA_CRL_PATH` based on the `ECA_CRL_PATH_SYNC_HOURS` option.

If the `ECA_CRL_CHECK` or `HADOOP_CRL_CHECK` option is not set to `DISABLE` (or 0) and the `ECA_CRL_PATH` option is not specified, NetBackup downloads the CRLs from the URLs that are specified in the CRL distribution point (CDP) and uses them to verify revocation status of the peer host's certificate.

Note: For validating the revocation status of a virtualization server certificate, the `VIRTUALIZATION_CRL_CHECK` option is used.

For validating the revocation status of a Hadoop server certificate, the `HADOOP_CRL_CHECK` option is used.

Table 4-49 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients. If certificate validation is required for VMware, Red Hat Virtualization servers, Nutanix AHV, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA). If certificate validation is required for VMware, Red Hat Virtualization servers, or Hadoop, this option must be set on the NetBackup primary server and respective access or backup hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).

How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	
	For information about these commands, see the NetBackup Commands Reference Guide.
	
	Use the following format to specify a path to the CRL directory:
	
	`ECA_CRL_PATH = Path to the CRL directory`
	
	For example:
	
	`ECA_CRL_PATH = /usr/eca/crl/eca_crl_file.crl`
	
	If you use this option on a Flex Appliance application instance, the path must be `/mnt/nbdata/hostcert/crl`.

Equivalent UI property	No equivalent exists.

ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients

The `ECA_CRL_PATH_SYNC_HOURS` option specifies the time interval in hours to update the Certificate revocation lists (CRL) in the NetBackup CRL cache with the CRLs in the directory that is specified for the `ECA_CRL_PATH` configuration option.

See "ECA_CRL_PATH for NetBackup servers and clients" on page 184.

The `ECA_CRL_PATH_SYNC_HOURS` option is not applicable if CDP is used for CRLs.

By default, CRLs in the cache are updated every one hour.

During host communication, revocation status of the external certificate is validated against the CRLs from the CRL cache.

Table 4-50 ECA_CRL_PATH_SYNC_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_PATH_SYNC_HOURS = Number of hours` Minimum number of hours that you can specify - 1 hour Maximum number of hours that you can specify - 720 hour The default value is one hour.
Equivalent UI property	No equivalent exists.

ECA_CRL_REFRESH_HOURS for NetBackup servers and clients

The `ECA_CRL_REFRESH_HOURS` option specifies the time interval in hours to download the CRLs from the URLs that are specified in the peer host certificate's CRL distribution points (CDP).

The `ECA_CRL_REFRESH_HOURS` option is applicable when you use CDP for CRLs.

See "ECA_CRL_PATH for NetBackup servers and clients" on page 184.

After the specified time interval, CRLs of the certificate authority are downloaded from the URLs that are available in CDP.

By default, the CRLs are downloaded from the CDP after every 24 hours.

Table 4-51 ECA_CRL_REFRESH_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-51 ECA_CRL_REFRESH_HOURS information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_CRL_REFRESH_HOURS = Number of hours` Minimum number of hours that you can specify - 0 hour, which indicates that CRLs from the CDP are not periodically downloaded. Maximum number of hours that you can specify - 4380 hours The default value for the option is 24 hours. **Note:** CRLs are also downloaded from the CDP during host communication if they are expired or not available in the CRL cache, irrespective of the time interval set for the `ECA_CRL_REFRESH_HOURS` option.
Equivalent UI property	No equivalent exists.

ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients

When NetBackup is configured to use the certificates that an external CA has signed, such certificates are automatically enrolled with the primary server during host communication. If you want to disable automatic enrollment of such certificates, set the `ECA_DISABLE_AUTO_ENROLLMENT` to '1'.

When automatic enrollment is disabled, you can enroll the external certificates manually using the `nbcertcmd -enrollCertificate` command.

A certificate must be enrolled with the primary server before it can be used for host communication.

By default, automatic certificate enrollment is enabled.

Table 4-52 ECA_DISABLE_AUTO_ENROLLMENT information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 4-52 ECA_DISABLE_AUTO_ENROLLMENT information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: `ECA_DISABLE_AUTO_ENROLLMENT = 1`
Equivalent UI property	No equivalent exists.

ECA_DR_BKUP_WIN_CERT_STORE for NetBackup servers and clients

The `ECA_DR_BKUP_WIN_CERT_STORE` option specifies whether you want to take a backup of the Windows certificate store information during catalog backup or not.

By default, Windows certificate store information is backed up during catalog backup.

Note: If the Windows certificate store information is not exportable, it cannot be backed up during catalog backup.

Table 4-53 ECA_DR_BKUP_WIN_CERT_STORE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. If you do not want the catalog backup operation to take a backup of the Windows certificate store information, use the following format: `ECA_DR_BKUP_WIN_CERT_STORE = NO`
Equivalent UI property	No equivalent exists.

MANAGE_WIN_CERT_STORE_PRIVATE_KEY option for NetBackup primary servers

The MANAGE_WIN_CERT_STORE_PRIVATE_KEY option lets you disable the automatic permission management of the private key of the certificate in Windows Certificate Store.

This option is applicable for Windows Certificate Store and only when the NetBackup services are running in the Local Service account context.

When NetBackup services are running in the Local Service account context, the services need to have permissions to read the private key for certificate in Windows Certificate Store.

When the MANAGE_WIN_CERT_STORE_PRIVATE_KEY option is set to Automatic, the NetBackup service that is running in the privileged user account context grants access to all other NetBackup services for reading the private key whenever required.

By default, permissions for the private key are automatically managed. When the MANAGE_WIN_CERT_STORE_PRIVATE_KEY option is set to Disabled, the permissions of the private key need to be managed manually.

Note: It is not recommended to set the MANAGE_WIN_CERT_STORE_PRIVATE_KEY option to Disabled.

To manually update the permissions when this option is Disabled, run the following command:

```
nbcertcmd -setWinCertPrivKeyPermissions -reason audit reason -force
```

Refer to the NetBackup Commands Reference Guide for more details on the command-line options.

Table 4-54 MANAGE_WIN_CERT_STORE_PRIVATE_KEY information

Usage	Description
Where to use	On NetBackup primary server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option. For information about these commands, see the NetBackup Commands Reference Guide. Use the following format: MANAGE_WIN_CERT_STORE_PRIVATE_KEY = Automatic

Table 4-54 MANAGE_WIN_CERT_STORE_PRIVATE_KEY information *(continued)*

Usage	Description
Equivalent NetBackup web UI property	No equivalent exists.

Guidelines for managing the primary server NetBackup catalog

Consider the following:

- Back up the catalog.
  Catalog backup can be performed while regular backup activity takes place. It is a policy-based backup. It also allows for incremental backups, which can significantly reduce catalog backup times for large catalogs.

  Warning: Failure to backup the primary server NetBackup catalog may result in data loss if a catastrophic failure occurs to the file systems housing the various parts of the catalog.

  Note: Cohesity recommends schedule-based, incremental catalog backups with periodic full backups.

  Be cautious in using Accelerator full backups daily as a replacement for daily incremental backups. While Accelerator full backups are quick to run, the catalog size will be a full catalog backup instead of an incremental and can grow quickly in size. Backups of client data that contain millions of small files in combination with the use of Accelerator and frequent full backups can also cause the catalog to bloat.

- Store the catalog on a separate file system.
  The primary server NetBackup catalog can grow quickly depending on backup frequency, retention periods, and the number of files being backed up. With the catalog data on its own file system, catalog growth does not affect other disk resources, root file systems, or the operating system.
  Information is available on how to move the catalog.
  The following directories and files that are related to the catalog can also be moved. Using an SSD device also improves performance:

  On a Linux/UNIX host:

- `/usr/openv/netbackup/db/error` (directory)
- `/usr/openv/netbackup/db/images` (directory)
- `/usr/openv/netbackup/db/jobs` (directory)
- `/usr/openv/netbackup/db/rb.db` (file)

On a Windows host:

- `C:\Program Files\VERITAS\NetBackup\db\error` (directory)
- `C:\Program Files\VERITAS\NetBackup\db\images` (directory)
- `C:\Program Files\VERITAS\NetBackup\db\jobs` (directory)
- `C:\Program Files\VERITAS\NetBackup\db\rb.db` (file)

- Change the location of the NetBackup relational database files.
  The location of the NetBackup database files can be changed for better performance. For example, you may want to change the database location if the default location is running short of space. Using an SSD device also can improve performance.
  The following directories and files that are related to the catalog can also be moved:

  On a Linux/UNIX host:

  - `/usr/openv/tmp` (directory)
  - `/usr/openv/var` (directory)
  - `/usr/openv/db/data` (directory)
  - `/usr/openv/db/staging` (directory)

  On a Windows host:

  - `C:\Program Files\VERITAS\NetBackup\Temp` (directory)
  - `C:\Program Files\VERITAS\NetBackup\var` (directory)
  - `C:\Program Files\VERITAS\NetBackupDB\data` (directory)
  - `C:\Program Files\VERITAS\NetBackupDB\staging` (directory)

  Refer to the procedure in the section *Moving a database after installation* in the *NetBackup Administrator's Guide, Volume I*.

- Set a delay to compress the catalog.
  The default value for this parameter is 0, which means that NetBackup does not compress the catalog. As your catalog increases in size, you may want to use a value between 10 days and 30 days for this parameter. When you restore old backups, NetBackup automatically uncompresses the files as needed, with minimal performance effect.

- Adjust the batch size for sending metadata to the catalog.
  This setting affects overall backup performance, not the performance of catalog backups.
- Best practices for primary server NetBackup catalog layout:
  https://support.cohesity.com/s/article/article-100003918

About protecting the MSDP catalog

To increase availability, NetBackup provides a two-tier approach to protect the MSDP catalog, as follows:

Daily shadow copies	NetBackup automatically creates copies of the MSDP catalog. See "About the MSDP shadow catalog" on page 192.
Catalog backup policy	Cohesity provides a utility that you can use to configure a NetBackup policy that backs up the MSDP catalog. See "About the MSDP catalog backup policy" on page 196.

About the MSDP shadow catalog

The NetBackup Deduplication Manager automatically creates a *shadow copy* of the catalog daily. The Deduplication Manager also builds a transaction log for each shadow copy. If NetBackup detects corruption in the MSDP catalog, the Deduplication Manager restores the catalog automatically from the most recent shadow copy. That restore process also plays the transaction log so that the recovered MSDP catalog is current.

By default, the NetBackup Deduplication Manager stores the shadow copies on the same volume as the catalog itself. Cohesity recommends that you store the shadow copies on a different volume.

Warning: You can change the path only during initial MSDP configuration only. If you change it after MSDP backups exist, data loss may occur.

See "Changing the MSDP shadow catalog path" on page 193.

The NetBackup Deduplication Manager creates a shadow copy at 0340 hours daily, host time. To change the schedule, you must change the scheduler definition file.

See "Changing the MSDP shadow catalog schedule" on page 194.

By default, the NetBackup Deduplication Manager keeps five shadow copies of the catalog. You can change the number of copies.

See "Changing the number of MSDP catalog shadow copies" on page 195.

Changing the MSDP shadow catalog path

You can change the location of the catalog shadow copies. It is recommended that you store the copies on a different volume than both the *storage_path* and the *database_path*. (If you configured a separate path for the deduplication database, the paths are different.)

NetBackup stores the MSDP catalog shadow copies in the following location:

UNIX: */database_path*/databases/catalogshadow

Windows: *database_path*\databases\catalogshadow

Warning: You can change the shadow catalog path during initial MSDP configuration only. If you change it after MSDP backups exist, data loss may occur.

See "About protecting the MSDP catalog" on page 192.

To change the MSDP catalog shadow path

1. Open the following file in a text editor:

   UNIX: */storage_path*/etc/puredisk/spa.cfg

   Windows: *storage_path*\etc\puredisk\spa.cfg

2. Find the `CatalogShadowPath` parameter and change the value to the wanted path.

   The volume must be mounted and available.

3. After your changes, save the file.

4. Create the `.catalog_shadow_identity` file in the catalog shadow path that you have specified in step 1.

   Note: There is a period (.) in front of the file name that denotes a hidden file.

   ---

5. Restart the NetBackup Deduplication Manager (`spad`).

6 Create the shadow catalog directories by invoking the following command on the MSDP storage server:

UNIX: `/usr/openv/pdde/pdcr/bin/cacontrol --catalog backup all`

Windows: *`install_path`*`\Veritas\pdde\cacontrol --catalog backup all`

7 If an MSDP catalog backup policy exists, update the policy with the new shadow catalog directories. To do so, invoke the following command on the MSDP storage server:

UNIX: `/usr/openv/pdde/pdcr/bin/drcontrol --update_policy --policy` *`policy_name`*

Windows: *`install_path`*`\Veritas\pdde\drcontrol --update_policy --policy` *`policy_name`*

Changing the MSDP shadow catalog schedule

NetBackup automatically creates a copy of the MSDP catalog at 0340 hours daily, host time. You can change the default schedule.

See "About protecting the MSDP catalog" on page 192.

To change the MSDP shadow catalog schedule

1. Open the following file in a text editor:

   UNIX: `/database_path/databases/spa/database/scheduler/5`

   Windows: `database_path\databases\spa\database\scheduler\5`

   By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different.

   The contents of the file are similar to the following line. The second section of the line (`40 3 * * *`) configures the schedule.

   ```
   CatalogBackup|40 3 * * *|21600|32400|
   ```

2. Edit the second section of the file (`40 3 * * *`). The schedule section conforms to the UNIX `crontab` file convention, as follows:

   ```
   40 3 * * *
   ┬  ┬ ┬ ┬ ┬
   │  │ │ │ │
   │  │ │ │ │
   │  │ │ │ └──── Day of week (0 - 7, Sunday is both 0 and 7, or use
   │  │ │ │       sun, mon, tue, wed, thu, fri, sat; asterisk (*) is
   │  │ │ │       every day)
   │  │ │ └─────────── Month (1 - 12; asterisk (*) is every month)
   │  │ └──────────────── Day of month (1 - 31; asterisk (*) is every
   │  │                   day of the month)
   │  └──────────────────── Hour (0 - 23; asterisk (*) is every hour)
   └─────────────────────── Minute (0 - 59; asterisk (*) is every
                            minute of the hour)
   ```

3. After your changes, save the file.

4. Restart the NetBackup Deduplication Manager (`spad`).

Changing the number of MSDP catalog shadow copies

NetBackup keeps five shadow copies of the MSDP catalog. You can change the number of copies.

See "About protecting the MSDP catalog" on page 192.

To change the number of MSDP catalog shadow copies

1. Open the following file in a text editor:

   UNIX: `/storage_path/etc/puredisk/spa.cfg`

   Windows: `storage_path\etc\puredisk\spa.cfg`

2. Find the `CatalogBackupVersions` parameter and change the value to the wanted number of shadow copies. The valid values are 1 to 256, inclusive.
3. After your changes, save the file.
4. Restart the NetBackup Deduplication Manager (`spad`).

About the MSDP catalog backup policy

Cohesity recommends that you protect the MSDP catalog by backing it up. A NetBackup catalog backup does not include the MSDP catalog. The NetBackup Deduplication Catalog Policy Administration and the Catalog disaster recovery utility (the `drcontrol` utility) configure a backup policy for the MSDP catalog. The policy also includes other important MSDP configuration information.

The MSDP catalog backups provide the second tier of catalog protection. The catalog backups are available if the shadow copies are not available or corrupt.

The following are the attributes for the catalog backup policy that the `drcontrol` utility creates:

Schedule	Weekly **Full Backup** and daily **Differential Incremental Backup**.
Backup window	6:00 A.M. to 6:00 P.M.
Retention	2 weeks

Backup selection

The following are the default catalog paths.

UNIX:

```
/database_path/databases/catalogshadow
/storage_path/etc
/database_path/databases/spa
/storage_path/var
/usr/openv/lib/ost-plugins/pd.conf
/usr/openv/lib/ost-plugins/mtstrm.conf
/database_path/databases/datacheck
```

Windows:

```
database_path\databases\catalogshadow
storage_path\etc
storage_path\var
install_path\Veritas\NetBackup\bin\ost-plugins\pd.conf
install_path\Veritas\NetBackup\bin\ost-plugins\mtstrm.conf
database_path\databases\spa
database_path\databases\datacheck
```

By default, NetBackup uses the same path for the storage and the catalog; the *database_path* and the *storage_path* are the same. If you configure a separate path for the deduplication database, the paths are different. Regardless, the `drcontrol` utility captures the correct paths for the catalog backup selections.

You should consider the following items carefully before you configure an MSDP catalog backup:

- Do not use the **Media Server Deduplication Pool** as the destination for the catalog backups. Recovery of the MSDP catalog from its **Media Server Deduplication Pool** is impossible.
- Use a storage unit that is attached to a NetBackup host other than the MSDP storage server.
- Use a separate MSDP catalog backup policy for each MSDP storage server. The `drcontrol` utility does not verify that the backup selections are the same for multiple storage servers. If the backup policy includes more than one MSDP storage server, the backup selection is the union of the backup selections for each host.
- You cannot use one policy to protect MSDP storage servers on both UNIX hosts and Windows hosts.

UNIX MSDP storage servers require a Standard backup policy and Windows MSDP storage servers require an MS-Windows policy.

How to set up malware scanning

Table 4-55 describes a high level process for setting up malware scanning.

Table 4-55 Process for setting up malware scanning

Steps	Description
Step 1	Install or upgrade NetBackup software on the primary server, the media server, and MSDP storage server to version 10.0 or later. NetBackup Installation or Upgrade Guide
Step 2	For BYO setup, Instant access must be configured on MSDP storage server.
Step 3	On the scan host, configure any of the following malware tool: ■ NetBackup Malware Scanner (Avira) **Note:** (*Applicable only for Avira*) Avira is configured automatically when using the automated scripts as described in Step 4 below. ■ Symantec Protection Engine ■ Microsoft Defender Antivirus ■ Trend Micro Malware Scanner **Note:** Ensure that the host user has required permission to scan with configured malware tool and is able to access the mount on the storage server.
Step 4	Malware scanning feature requires additional configurations on scan host. The scan host configuration can be performed through automated scripts or manually. ■ Automated scripts: ■ Manual configuration: Scenario based scan host configuration: ■ **For Agentless host** ■ **For NetBackup client as the scan host**
Step 5	On the NetBackup Web UI, configure the malware detection settings.

Prerequisites for a scan host

A scan host is a host machine that has the required malware tool configured. Once it is integrated with NetBackup, NetBackup initiates scanning on the scan host.

Ensure that you meet the following prerequisites:

- The minimum required configuration for the scan host is 8 CPU and 32-GB RAM.
- The malware tool must be installed and configured.
- For the supported operating systems of the scan host, refer to the Software Compatibility List.
- The scan host must have a share type configured, that is, an NFS or an SMB client.
- If the scan host connectivity type is **Agentless host**:
  - NetBackup footprint is not required on the scan host. The existing systems with the NetBackup client or media server can be used as scan host, too.
  - The scan host must be reachable from the media server over SSH.

    Note: The SSH connection to the scan host from the media server must be successful. You can verify this connection by running the following command from the media server:

    ```
    ssh scanuser@scanhost
    ```

  If the scan host connectivity type is **NetBackup client**:
  - NetBackup footprint is required on the scan host.
  - The NetBackup primary server and the media server providing the Instant Access mounts must be reachable from the NetBackup client.
  - By default, the NetBackup client scan host would be in a deactivate state. After adding NetBackup client scan host to scan host pool you must activate the scan host.
- The malware tool uses the temporary location to store the files that are created during the malware scan. The path of the temporary location is configured in the web UI in the **Malware global settings**. Ensure that the user has write permissions to this path.
  For archive scanning purposes, it is recommended to have the free disk space of 10 GB on the scan host.

Note: (*Applicable for NetBackup version 10.0 and later*) Any other malware scanner tools that are installed on the scan host with on-access/real time protection enabled can interfere with backup scanning. Disable or add NFS/SMB mounts on the scan host to the exclusion list of the scanner.

For example, on a Windows scan host, the user must disable the **Real time protection** option of the Windows Defender while the malware scan is in progress.

- Depending on the platform, ensure that the following additional prerequisites are met:
  Windows:
  Linux:

Note: It is recommended to keep only the required ports open for malware scanning.

Allow NFS/SMB read from the NetBackup storage server. Refer to *NetBackup Network Ports Reference Guide*.

Allow SSH from the NetBackup media server (used for connecting to scan host).

Allow Malware signature updates. The updates that are needed depend on the malware scanner that is used. For NetBackup Malware Scanner, the update happens over HTTPS (https://oem.avira-update.com/update).

Configure a new scan host pool

To configure a new scan host pool

1. On left, select **Detection and reporting > Malware detection**.
2. At the top right, select **Malware detection settings > Manage malware scanner host pools** to go to the host pool list page.
3. Select **Add** to add a new host pool.
4. Enter the details such as **Host pool name**, **Malware scanner**, **Host type**, and **Type of share**.
5. Select **Save and add hosts**.

About backup anomaly detection

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

The following backup job metadata, attributes, or features are verified during backup anomaly detection:

- Backup image size
- Number of backup files
- Data that is transferred in KB
- Deduplication rate
- Backup job completion time

Any unusual deviation in these backup job attributes is considered to be an anomaly and is notified using the NetBackup web UI.

Starting with 10.4, NetBackup can detect anomalies for Oracle workload only for the image size attribute. If an Oracle workload job fails multiple times with status code 5407, NetBackup flags it as an anomaly.

Workflow of backup anomaly detection and notification

The workflow of the backup anomaly detection and notification is as follows:

Table 4-56 Workflow

Step	Description
Step 1	Install or upgrade NetBackup software on the primary server and the media server. See the NetBackup Installation or Upgrade Guide.
Step 2	Enable the primary server to detect backup anomalies. By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.
Step 3	Configure anomaly detection settings using the NetBackup web UI. See “Configure backup anomaly detection settings” on page 203.
Step 4	View the anomalies using the NetBackup web UI. See “View backup anomalies” on page 206.

Detecting backup anomalies on the primary server

This topic provides the procedure to enable the primary server to detect backup anomalies.

To enable the primary server to detect backup anomalies

1. Install the NetBackup primary server software on your system (or upgrade the primary server software).

   After the installation, the following configurations are automatically done on the primary server:

   - The `NetBackup Anomaly Detection Management` service (`nbanomalymgmt`) is started on the primary server.
     The anomaly detection and alert services do not run by default.

     Note: The `NetBackup Anomaly Detection Management` service stops if the proxy server takes more than 45 minutes to connect to the primary server.

2. Configure the backup anomaly settings using the NetBackup web UI. NetBackup takes these settings into account during anomaly detection.

   See "Configure backup anomaly detection settings" on page 203.

   If any anomalies are detected, they are notified through the NetBackup web UI.

   See "View backup anomalies" on page 206.

Detecting backup anomalies on the media server

This topic provides the workflow and the procedure that enable the media server to detect backup anomalies.

Note: By default, the anomaly detection algorithm runs on the NetBackup primary server. If you see any impact on the primary server because of the anomaly detection process, you can configure a media server to detect anomalies.

To enable the media server to detect backup anomalies

1. Install the NetBackup media server software on your system (or upgrade the media server software).
2. On the primary server, add anomaly proxy server details. The proxy server should be the media server where you want the anomaly algorithms to be run.

   See "Configure backup anomaly detection settings" on page 203.
3. (Optional) If you want to preserve the data that the primary server has gathered earlier, do the following:
   - Ensure that the `nbanomalymgmt` service is disabled using the web UI.
   - Ensure that the `nbanomalymgmt` service on the media server is stopped.
   - Go to the following directory:
     On Windows: *`Install_Path`*`\NetBackup\var\global`
     On UNIX: `/usr/openv/var/global`
     The directory resides on the shared disk on a clustered primary server.
   - Copy the `NB_Anomaly.db`, `NB_Anomaly.db-shm`, and `NB_Anomaly-wal` files from the `anomaly_detection` folder on the primary server to the `anomaly_detection` folder on the media server.
     You can copy the `anomaly_config.conf` file to preserve the automatic malware scan settings.
   - Start the `nbanomalymgmt` service on the media server.
4. On the media server, start the `nbanomalymgmt` service manually. Use the following script:

   ```
   nbanomalymgmt -start
   ```
5. Configure the backup anomaly settings in the NetBackup web UI. NetBackup takes these settings into account during anomaly detection.

   See "Configure backup anomaly detection settings" on page 203.

   If any anomalies are detected, they are notified using the NetBackup web UI.

   See "View backup anomalies" on page 206.

Configure backup anomaly detection settings

After you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. Basic and advanced backup anomaly detection settings are available to be configured.

See "About backup anomaly detection" on page 200.

See "View backup anomalies" on page 206.

To configure backup anomaly detection settings

1. On the left, click **Detection and reporting > Anomaly detection.**
2. On the top right, click **Anomaly detection settings > Backup anomaly detection settings**.
3. Click **Edit** on the right to configure the following **Anomaly detection > Enable anomaly detection activities** settings:
   - **Enable only for unstructured data** - Enables anomaly detection for the following policy types: Standard, MS-Windows, NAS-Data-Protection, and Universal share.

     Note: This is the default configuration for fresh NetBackup 10.4 installation.

   - **Enable** - Enables anomaly detection for all policy types except for the ones that are excluded in the **Advanced settings > Disable policy type or specific features for machine learning**.
   - **Disable** - Disables anomaly detection in NetBackup for all workload types.
   - Click **Save**.

   In the case of NetBackup 10.4 upgrade, the value of the **Anomaly detection** option is set based on the previous setting.

   - If the option was set to **Enable anomaly data collection, detection service, and events** in the previous version, the option is set to **Enable** after the upgrade.
   - If the option was set to a value other than **Enable anomaly data collection, detection service, and events** in the previous version, the option is set to **Disable** after the upgrade.
4. Click **Edit** on the right to configure the **Anomaly detection > Enable automatic scan for imported copy** setting.
   - On the **Enable automatic scan for imported copy** pop-up screen, select the **Turn on automatic scan for imported copy** check box.
     After enabling the scan for imported copy from the web UI, you must do the following configurations in the `anomaly_config.conf` file:

     ```
     [AUTOMATED_MALWARE_SCAN_SETTINGS]
     SCAN_HOST_POOL_NAME=ScanHostPoolName
     ENABLE_ALL_CLIENTS=1
     TRIGGER_SCAN_FOR_LOW_SEVERITY=1
     ```

```
TRIGGER_SCAN_FOR_MEDIUM_SEVERITY=1
```

- Click **Save**.

5 Select **Edit** to modify the following **Basic Settings**:

- **Anomaly detection sensitivity**
  Use this setting to increase or decrease the sensitivity with which anomalies are detected. If the sensitivity is low, anomalies are detected based on less number of anomalous events.
  If the sensitivity is high, anomalies are detected based on a large number of anomalous events.
- **Data retention settings**
  Use this setting to specify how long you want to retain the anomaly data (in months).
- **Data gathering settings**
  Use this setting to specify the time interval (in minutes) after which the anomaly data is gathered for analysis.
- **Anomaly proxy server settings**
  Use this setting to specify the NetBackup media server where the anomalies are going to be processed. If not specified, the processing takes place on the primary server.
- Click **Save**.

6 Expand the **Advanced settings** section to configure the following settings:

- Click **Edit** on the right to configure the **Disable anomaly settings for clients** settings.
  Click **Save**.
- Click **Edit** on the right to configure the **Disable policy type or specific features for machine learning** settings.
  On the pop-up screen, all the policies are listed.
  Use the action menus to disable one or all of the following anomaly features for machine learning for the given policy: Backup files count, Data transferred, Deduplication ratio, Image size, and Total time.
  - **Disable all** - Use this option to disable all of the anomaly features for machine learning for the given policy.
  - **Disable specific features** - Use this option to select specific anomaly features that you want to disable for machine learning.
  - Click **Save**.
- Click **Edit** on the right to configure the **Suspicious file extension settings**.

- Select the **Turn on suspicious file extension detection** to enable NetBackup to detect files with suspicious file extensions.
  A malware such as ransomware attacks the data and encrypts it. After the file encryption, the ransomware renames the files with a specific extension such as `.lockbit`. NetBackup detects such known suspicious file extensions during backups and generates an anomaly.
- **Files with suspicious extensions (in %)**
  Select the percentage (1 to 50) of files with suspicious extensions from the **Percent** drop-down list, which is acceptable in your environment. When the percentage of the files with suspicious extensions exceeds this threshold, an anomaly is generated.

- You can add or remove the suspicious file extensions from the list.
- Click **Save**.

Client offline anomaly type

As part of backup anomaly detection, clients that are offline under suspicious circumstances (with error code 7647) are detected and anomalies are generated.

View backup anomalies

NetBackup can now detect anomalies in backup metadata. It can detect any unusual job data in the data backup flow. For example, it can detect a file count or a file size that is different than the usual count or size.

Consider the following example:

An anomaly of the image size type is displayed as 100MB (Usual 350MB, 450MB). This information implies that the current image size that is reported as anomaly is 100 MB. However, the usual image size range is 350 MB - 450 MB that is derived from the analysis of past data. Because of the significant difference between the current image size and usual image size range, NetBackup notifies it as an anomaly.

See “About backup anomaly detection” on page 200.

Note: Anomaly count of `0` indicates that there are no anomalies generated or that the anomaly detection services are not running.

To view backup anomalies

1 On the left, select **Detection and reporting > Anomaly detection > Backup anomalies**.

The following columns are displayed:

- Job ID - ID of the job for which the anomaly is detected
  All child jobs and the associated anomaly details are also shown when you expand the parent job.
- Severity - Severity of the anomalies that are notified for this job
- Asset name - Name of the NetBackup client where the anomaly is detected
- Summary - For the parent job, details like types of anomalies, number of anomalies, and increase or decrease in the number of anomalies are shown. For child jobs, types of anomalies are shown, such as Database corruption.
- Anomaly type - Type of the anomaly such as Image entropy, Job metadata, Suspicious file extension, Client offline
- Backup selection - The backup selection (client or file to be backed up) that is specified in the policy
- Policy name - The policy name of the associated backup job
- Policy type - The policy type of the associated backup job
- Schedule type - The schedule type of the associated backup job
- Impacted number of jobs - The number jobs for which anomalies are detected
- Review status - The anomaly status that indicates whether the detected anomaly is reported as a false positive or an actual anomaly, or it can be ignored.
- Last updated - The date and time when the anomaly status is updated

2 Select the job ID to see the job details in the Activity monitor. Expand a parent job to see the details of each child job.

3 You can perform the following actions on the anomaly record:

- Select **Report as false positive** if the anomaly is a false positive. Similar anomalies are not shown in the future.
  The **Review status** of the anomaly record appears as `False positive`.
- Select **Confirm as anomaly** when you want to take some action on the anomaly condition.
  The **Review status** of the anomaly record appears as `Anomaly`.
- Select **Mark as ignore** when you can ignore the anomaly condition.
  The **Review status** of the anomaly record appears as `Ignore`.

Send audit events to system logs

You can send NetBackup audit events to system logs. You must have the NetBackup Security Administrator role or similar RBAC permissions to perform this task.

By default, NetBackup sends the audit events to system logs in native format. You can now export audit events with the Open Cybersecurity Schema Framework (OCSF) format to Security Information and Event Management (SIEM) platforms.

See this article for more information.

Use the `SYSLOG_AUDIT_USE_OCSF_FORMAT` configuration option to send the NetBackup audit events to system logs in the OCSF format.

To send audit events to system logs

1. Open the NetBackup web UI.
2. On the left, select **Security > Security events**.
3. On the top right, click **Security event settings**.
4. Enable the **Send the audit events to the system logs** option.
5. Select **Select audit event** categories. Then select the audit categories for which you want to send the audit events to the system logs.

   To send audit events for all audit categories to the system logs, select the **Audit event categories** check box.
6. Select **Save**.

   You can view NetBackup audit events in the system logs. For example:

   On a Windows system, use **Windows Event Viewer** to view NetBackup audit events.

   On a Linux system, you can view the system logs on the configured location.

Send audit events to log forwarding endpoints

You can send NetBackup audit events to log forwarding endpoints.

To send audit events to log forwarding endpoints

1. On the left, select **Security > Security events**.
2. On the top right, select **Security events settings**.
3. Enable the **Send the audit events to log forwarding endpoints** option.

   After you enable the option, the **Select endpoints and categories** option displays.

4. Select the **Select endpoints and categories** option to see the log forwarding endpoints that are configured in your environment and the available audit categories.

   Example of an endpoint: Azure Sentinel.

5. Select the appropriate log forwarding endpoints.
6. Select the **Select audit event categories** option.
7. Select the categories of the audit events that you want to forward to the selected endpoints. For example, Alert, Anomaly, etc.
8. After you select your log forwarding endpoint, the options to specify the associated credentials display. You can either add new credentials for the endpoint or select the existing credentials.

Display a banner to users when they sign in

You can configure a sign-in banner that displays each time that any user signs in to the NetBackup web UI. A different banner can be configured for any primary server. This banner can also require the user to agree to the terms of service before the user signs in.

To display a banner to users when they sign in

1. On the left, click **Security > User sessions**.
2. At the top right, click **User account settings**.
3. Turn on **Sign-in banner configuration** and click **Edit**.
4. Enter the text you want to use for the heading and the body of the message.
5. If you want to require the user to agree to the terms of service, select **Include "Agree" and "Disagree" buttons on the sign-in banner**.
6. Select **Save**.

   For active users, the updates are applied the next time the user signs in.

To remove the sign-in banner

1. On the left, click **Security > User sessions**.
2. At the top right, click **User account settings**.
3. Turn off **Sign-in banner configuration**
4. Select **Save**.

   For active users, the updates are applied the next time the user signs in.

Chapter 5

Steps to protect NetBackup Flex Scale

This chapter includes the following topics:

About NetBackup Flex Scale hardening

This chapter contains information on the NetBackup Flex Scale features that can help to secure your data protection infrastructure. For more detailed information

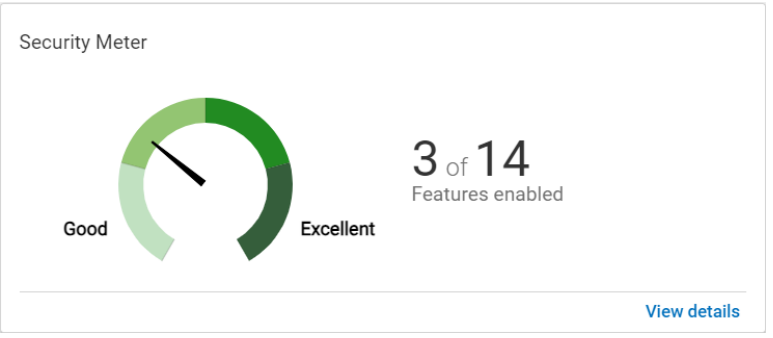
about NetBackup Flex Scale security, see the *Veritas NetBackup Flex Scale Administrator's Guide*.

About the security meter

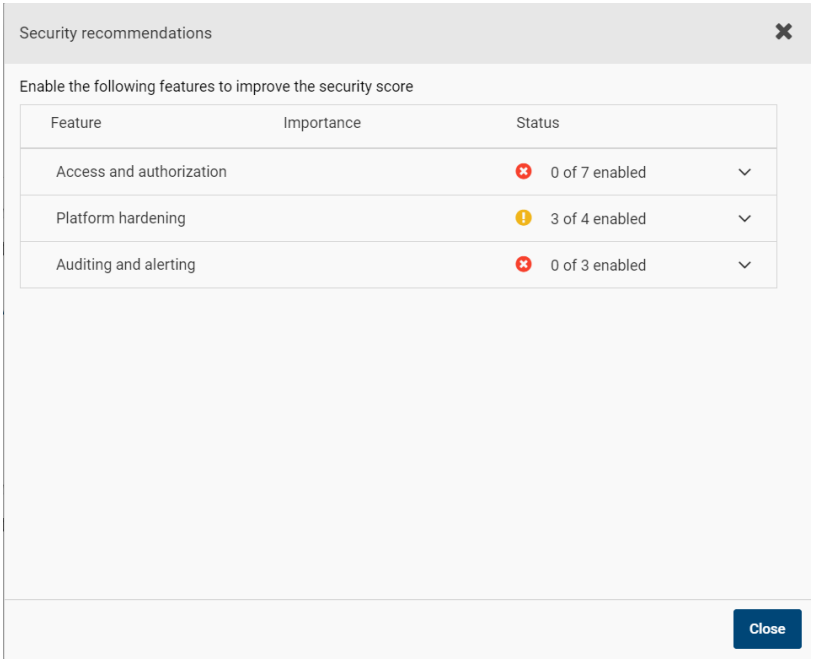
NetBackup Flex Scale includes a security meter to view and configure the appliance security settings from one location. The security meter provides security insights and recommendations to improve the appliance security. The security meter keeps a track of the security settings and shows you a list of available security features with quick links to configure them. The security meter displays the current security index from good to excellent based on how many security features are turned on. Built-in security features are turned on and shown as **Enabled** in the security meter.

The security meter can be found on the appliance dashboard. Only a user with an Appliance administrator role can view and manage the settings from the security meter.

The following figure shows the security meter that is displayed on the appliance dashboard:



The following figure shows all the appliance security settings that you can track and manage:



STIG overview for NetBackup Flex Scale

The Security Technical Implementation Guide (STIG) provides technical guidance for increasing the security of information systems and software to help prevent malicious computer attacks. This type of security is also referred to as hardening.

NetBackup Flex Scale uses STIG to meet security requirements as per the Defense Information Systems Agency (DISA) profile:

`STIG for Red Hat Enterprise Linux 8 Security Technical Implementation Guide - Version 1, Release 10`

The STIG option is enabled at cluster level. If the STIG option is enabled, the STIG rules are enforced on all the nodes in a cluster.

NetBackup Flex Scale also supports DISA's Application Security and Development STIG Version 5, Release 3.

STIG-compliant password policy rules

To comply with the Security Technical Implementation Guide (STIG), NetBackup Flex Scale automatically enforces a higher security password policy when the STIG option is enabled. After the STIG option is enabled, all current user passwords that

were created under the default policy remain valid. When you change any user passwords, the STIG-compliant policy rules must be followed.

The STIG-compliant password policy rules are listed below:

Password complexity

- Minimum characters: 15
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 1
  The permitted special characters are: ~!@#$%^&_+–=[]{},.<>¦
- Minimum character classes: 4
- Maximum consecutive repeating characters: 2
- Maximum consecutive repeating characters of the same type: 4
- Minimum number of different characters: 8
- No whitespaces.
- Dictionary words are not allowed

Password age

- Days after which a password expires: 60
- Minimum days before a password can be changed: 1
- Days before a password must be changed: 60
- The previous seven passwords cannot be reused.

Password lockout

- Number of incorrect login attempts before lockout: 3
- Time before locked account is reenabled (seconds): 604800
- Time between login failures before account lockout (seconds): 900

Enabling STIG for NetBackup Flex Scale

With NetBackup Flex Scale version 3.5, you can enable STIG hardening rules for increased security. These rules are based on the following profile from the Defense Information Systems Agency (DISA):

```
STIG for Red Hat Enterprise Linux 8 Security Technical Implementation
Guide - Version 1, Release 10
```

After the STIG option is enabled:

- A STIG-compliant password policy is automatically enforced. All current user passwords that were created under the default password policy remain valid. Once a password expires, you must follow the STIG-compliant policy rules when you change the password.
  See "STIG-compliant password policy rules" on page 212.
- The STIG default login banner is displayed when you log in to the NetBackup Flex Scale UI and the NetBackup Administration Console. View the **Alert! Accessing Information System** window and click **Continue** to proceed.

Review the following guidelines before enabling STIG:

- When you enable STIG, the STIG option is configured for all the nodes in a cluster. The cluster must be configured before you enable the STIG option.
- The STIG option does not allow individual rule control.
- Before you enable STIG, it is recommended that you complete the following prerequisites. However, not completing the prerequisites does not prevent you from enabling STIG. You can complete these requirements after you enable the STIG option.
  - Configure at least two NTP servers for the cluster.
  - Configure at least two DNS servers for the cluster.
  - Configure an SMTP server to enable notifications.
- After the STIG option is enabled, a factory reset is required to disable the associated rules. You cannot disable the option using the UI or the REST APIs.
- Cohesity recommends that you do not perform any other tasks while the STIG operation is in progress.
- If site-based disaster recovery is configured, ensure that both the primary and the secondary clusters have similar STIG configuration. If STIG is enabled for the primary cluster, the STIG option must be enabled for the secondary cluster. Similarly, if STIG is not enabled for the primary cluster, do not enable STIG for the secondary cluster.

Enabling STIG using the NetBackup Flex Scale web interface

To enable the STIG hardening rules, complete the following steps:

1. Use any one of the following options to log in using the user account that you created:
   - Use a user account with both Appliance Administrator and NetBackup Administrator role, or a user account with only an Appliance administrator

role to log in to the NetBackup Flex Scale web interface `https://`*`ManagementServerIPorFQDN`*`/webui` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings**.

- Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management console `https://`*`ManagementServerIPorFQDN`*`:14161` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings**.

Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

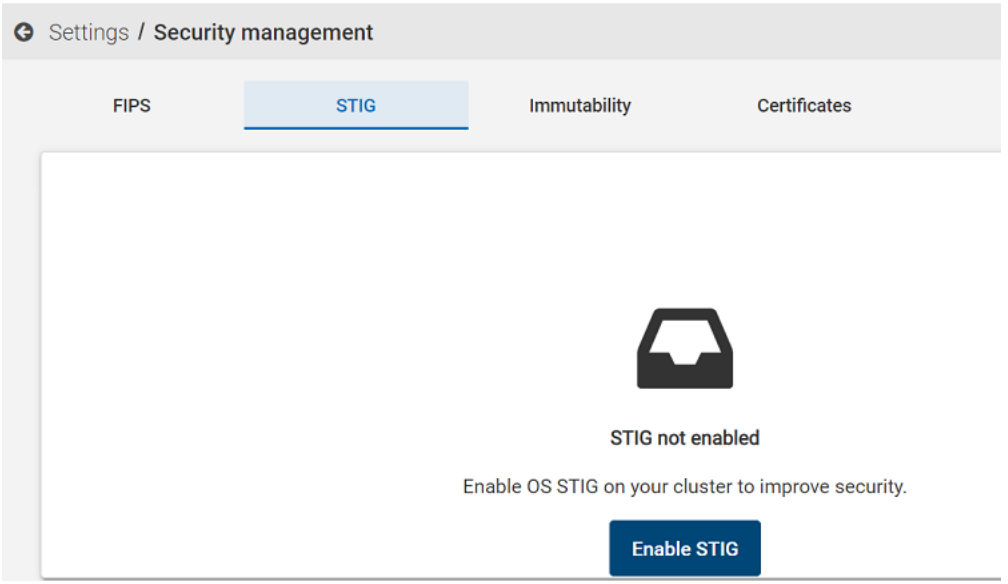
---

2 Click **Security management**.

3 On the **STIG** tab, click **Enable STIG**.

If the prerequisites are not met, you are prompted to resolve the errors. However you can choose to ignore these errors and proceed by clicking **Continue**. You can complete the prerequisites later after you enable the STIG option. If the requirements are met, review the displayed guidelines and click **Enable**.

Note: Do not perform any other tasks until the STIG enable operation is complete.



4 To monitor the progress, click **View details** on the **Security** page. The ongoing and completed tasks for the operation are also displayed in **Recent activity**.

After the operation is complete, you can view the STIG status for all the cluster nodes. If STIG is enabled for a node, the status is displayed as **Enabled**. If the STIG option cannot be enabled for a node, the status is displayed as **Not Enabled**, and if the node status cannot be retrieved because the node is stopped, shut down, or not reachable, the status is displayed as **Unknown**.

For nodes that display **Unknown** status, you can enable the STIG option again or wait for the node to automatically synchronize its status with the cluster after the node is up.

If some of the STIG rules fail or you make any updates to the cluster settings or configuration, you can enforce the STIG rules again on the nodes where the STIG option is already enabled by clicking **Enable STIG**.

Enabling STIG using REST APIs

You can use the following API to enable STIG:

```
PATCH /api/appliance/v1.0/security/stig
```

You can find the REST APIs at `https://`*`ManagementServerIPorFQDN`*`:14161/swagger/infra/v1.0/` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the management server and API gateway during the cluster configuration. For more details about the APIs, see the NetBackup Flex Scale APIs on SORT.

Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

Viewing the NetBackup Flex Scale STIG status

You can use the NetBackup Flex Scale web interface or the REST APIs to view the STIG status.

Viewing the status using the REST APIs

You can find the RESTful APIs at `https://`*`ManagementServerIPorFQDN`*`:14161/swagger/infra/v1.0/` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration.

Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

If you are using IPv6 addresses, use the following URL syntax:

`https://[`*`ManagementServerIP`*`]:14161/swagger/infra/v1.0`

Use the following API to view the STIG status:

```
GET /api/appliance/v1.0/security/stig
```

Viewing the status in the web interface

1. Use any one of the following options to log in using the user account that you created:

   - Use a user account with both Appliance Administrator and NetBackup Administrator role, or a user account with only an Appliance administrator role to log in to the NetBackup Flex Scale web interface `https://`*`ManagementServerIPorFQDN`*`/webui` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings > Security management**.
   - Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management console `https://`*`ManagementServerIPorFQDN`*`:14161` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > Security management**.

     Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

2. Click the **STIG** tab.

   The STIG status for all the cluster nodes is displayed:

   - **Enabled**: The STIG option was successfully enabled for the node.
   - **Not Enabled**: The STIG option is not enabled for the node.
   - **Unknown**: The node status cannot not be retrieved because the node is stopped, shut down, or not reachable.

FIPS overview for NetBackup Flex Scale

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for validating cryptography modules. The FIPS 140-2 standard specifies the security requirements for cryptographic modules and applies to both the hardware and the software components. It also describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

For more information about the FIPS 140-2 standard and its validation program, see the following links:

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

The NetBackup Flex Scale Cryptographic Module is FIPS validated. Starting with NetBackup Flex Scale 3.5, FIPS 140-2 standard is enabled with the default factory settings for the Veritas Optimized Operating System (VxOS). After FIPS for VxOS is enabled, the `sshd` uses the following FIPS approved ciphers:

- aes128-ctr
- aes192-ctr
- aes256-ctr

The FIPS 140-2 standard is enabled for NetBackup MSDP when you create a NetBackup Flex Scale cluster.

Note: You cannot disable the FIPS option for VxOS or for NetBackup MSDP.

Starting with NetBackup Flex Scale version 3.2, the application layer is FIPS-compliant.

Viewing the NetBackup Flex Scale FIPS status

You can use the NetBackup Flex Scale web interface or the REST APIs to view the FIPS status. The FIPS 140-2 standard is enabled with the default factory settings for the Veritas Operating System (VxOS) and for NetBackup MSDP when you create a NetBackup Flex Scale cluster.

Viewing the status using the REST APIs

You can find the RESTful APIs at
`https://`*`ManagementServerIPorFQDN`*`:14161/swagger/infra/v1.0/` where

ManagementServerIPorFQDN is the public IP address or FQDN that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration.

Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

If you are using IPv6 addresses, use the following URL syntax:

`https://[ManagementServerIP]:14161/swagger/infra/v1.0`

Use the following API to view the FIPS status:

```
GET /api/appliance/v1.0/security/fips
```

Viewing the status in the web interface

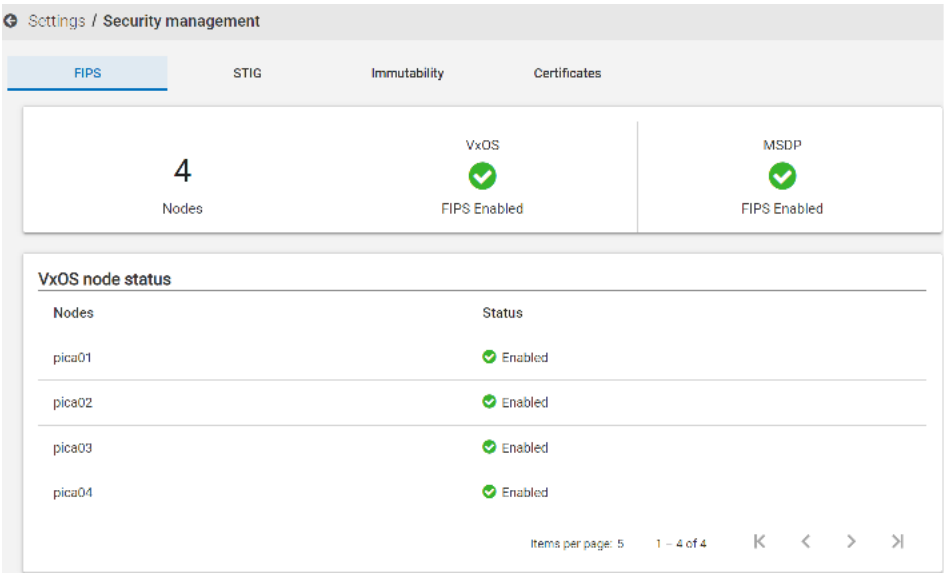
1. Use any one of the following options to log in using the user account that you created:

   - Use a user account with both Appliance Administrator and NetBackup Administrator role, or a user account with only an Appliance administrator role to log in to the NetBackup Flex Scale web interface `https://ManagementServerIPorFQDN/webui` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings > Security management**.
   - Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management console `https://ManagementServerIPorFQDN:14161` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > Security management**.

Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

2 Click the **FIPS** tab.

The FIPS status for VxOS and NetBackup MSDP is displayed. You can also view the FIPS status for VxOS for each node in the cluster. For nodes that are unreachable or are stopped, the status is displayed as **Unknown**.



Managing the login banner

You can create a customized text banner that appears when you sign in to NetBackup Flex Scale UI, system console, or NetBackup UI. You can use the login banner to communicate various kinds of messages to users. Typical uses for the login banner include legal notices, warning messages, and company policy information.

Note: Ensure that you change the banner from the NetBackup Flex Scale infrastructure management UI or the NetBackup Flex Scale web UI. If you change the banner in the NetBackup UI, the changes are not reflected in NetBackup Flex Scale.

To set a login banner:

1. Use any one of the following options to log in using the user account that you created:

   - Use a user account with both Appliance Administrator and NetBackup Administrator role, or a user account with only an Appliance administrator role to log in to the NetBackup Flex Scale web interface `https://`*`ManagementServerIPorFQDN`*`/webui` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Cluster Management > Cluster settings > User management**.
   - Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management console `https://`*`ManagementServerIPorFQDN`*`:14161` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > User management**.

     Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

2. Click **Manage sign-in banner**.

   If a banner is already set, the Manage sign-in banner page displays the current banner.

3. On the Manage sign-in banner page, click **Edit**.

4. (Optional) Under **Sign-in banner heading**, enter the banner heading. The heading can be a maximum of 250 characters.

5 Under **Sign in banner text**, enter the text for the banner message. The message can be a maximum of 4000 characters.

6 To review the changes, click **Preview**.

7 To confirm the changes, click **Save**.

Changing the password policy

You can customize the password policies by setting rules for the passwords that are used by the NetBackup Flex Scale local users. You can set rules for password complexity, password age, and password lockout. Password complexity specifies the number and type of characters a password must include. Password age defines the duration for which the password is valid. Password lockout specifies the number of failed attempts because of incorrect usage of passwords after which a user is prevented from logging in to the account.

The default password policy for a local user is as follows:

Password complexity:

- Minimum characters: 8
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 1

Note: Ensure that you change the password policy from the NetBackup Flex Scale infrastructure management UI or the NetBackup Flex Scale web UI. If you change the password policy in the NetBackup UI, the changes are not reflected in NetBackup Flex Scale.

To edit the password policy:

1 Use any one of the following options to log in using the user account that you created:

- Use a user account with both Appliance Administrator and NetBackup Administrator role, or a user account with only an Appliance administrator role to log in to the NetBackup Flex Scale web interface `https://`*`ManagementServerIPorFQDN`*`/webui` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and

then in the left pane click **Cluster Management > Cluster settings > User management**.

- Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management console `https://`*`ManagementServerIPorFQDN`*`:14161` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server and API gateway during the cluster configuration, and then in the left pane click **Settings > User management**.

Note: If you access the NetBackup Flex Scale infrastructure management console by using the short host name from a node, set the DNS settings (name server, domain name, and search domain) or ensure that the entry for mapping the short host name to an IP address exists in the hosts file of the node.

---

2 Click **Manage password policy**.

3 On the Manage password policy page, click **Edit**.

4 If you want your password policy to comply with STIG, select **Reset to STIG default values** to fill in the default values for all the parameters.

5 Edit the parameters as required. To ignore a rule, leave the corresponding parameter blank. After making the changes click **Save**.

Table 5-1

Parameter	Description
Minimum characters	Minimum number of characters to include in a password
Minimum uppercase characters	Minimum number of uppercase characters to include in a password
Maximum repetitive characters of the same class	Maximum number of consecutive uppercase, lowercase, numeric, and special characters
Minimum numbers	Minimum number of numeric characters
Minimum special characters	Minimum number of special characters in a password

Table 5-1 *(continued)*

Parameter	Description
Minimum character classes	Minimum character classes to include in a password. Character classes include uppercase, lowercase, numeric, and special characters.
Minimum lowercase characters	Minimum number of lowercase characters
Maximum repetitive characters	Maximum number of characters that can be repeated in a password.
Character difference with old password	Number of characters the new password must differ by from the previous password
Days after which password can be changed	Number of days after which a password can be changed
Days after which password must be changed	Number of days after which a password must be changed
Days before warning message	Number of days before the password expires to display a warning
Minimum different passwords before allowing reuse	Number of unique passwords before a previous password can be reused
Number of incorrect login attempts before lockout	Number of failed login attempts after which the account gets locked
Time before locked account is reenabled	Duration in seconds the account remains locked
Time between login failures before account lockout	Number of seconds between consecutive failed login attempts

Support for immutability in NetBackup Flex Scale

Immutability support for backup images requires locking down the appliance and not permitting any operations that can lead to data destruction. When the appliance is placed in lockdown mode, administrators are prevented from making any changes to the operating system and the internal components.

Important features:

- Immutable data support with retention locking
- Retention lock deletion for backup images

- Restricted access to Remote Management Platform (HPE iLO)
- Transition between different modes
- Retention lock extension

About lockdown modes

Lockdown mode is one of the features of ransomware protection. The lockdown mode protects your cluster data from internal and external threats by securing all the external endpoints from unauthorized access. Access to all the services is protected and authenticated.

NetBackup Flex Scale 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 the 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, you must contact Veritas Technical Support to obtain a Support Key and temporarily unlock the appliance. This functionality prevents unauthorized changes even if a malicious user gains access to stolen credentials.
- It gives the appliance users options for managing WORM (Write Once Read Many) data. Your data is protected from being encrypted, modified, and deleted using WORM properties.

Different lockdown modes provide different level of granularity for WORM and retention. The NetBackup Flex Scale appliance support three lockdown modes.

- **Normal mode**:
  - This is the default mode of the cluster if the lockdown mode is not specified during installation.
  - In this mode, WORM and retention capabilities are disabled. User cannot create worm STU in this mode.
- **Enterprise mode**:
  - In this mode, WORM and data retention features are enabled.
  - User can choose to create WORM-enabled STU.
  - User has the option to remove the retention locks and expire image data.
  - User can extend the retention period but cannot reduce the retention period.

- The retention time period can be extended from the NetBackup primary container only if the user has the NetBackup administrator role.
- Retention can be disabled or retention lock can be removed using the MSDP Restricted Shell only if the user has the appliance administrator role.
- After removing the images retention locks from the MSDP Restricted Shell, the user still cannot expire images from the NetBackup Administration Console, but can expire the images from the NetBackup primary server using the following command:

  ```
  /usr/openv/netbackup/bin/admincmd/bpexpdate -backupid
  n155-h201.cdc.veritas.com_1631842421 -d 0 -copy 1
  -try_expire_worm_copy
  ```

- **Compliance mode**:
  - In this mode, WORM and data retention features are enabled.
  - The user can extend the retention period.
  - The user does not have the option to remove retention locks and expire image data before the predefined time.
  - Once appliance lockdown mode is set to compliance, user does not have the option to delete data until it is expired.

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

Selecting or changing the lockdown mode

The user can select the lockdown mode during initial configuration. After cluster configuration, user has the option to see/change the lockdown mode using both GUI and REST APIs. The lockdown modes can be switched only if the engines are healthy. The user can switch between the following modes without any restriction:

- From normal to enterprise mode
- From normal to compliance mode
- From enterprise to compliance mode

The user can set minimum and maximum retention time for backup images for enterprise and compliance mode only. Creation of images with retention time less than the minimum retention time or greater than the maximum retention time is not allowed. This minimum and maximum retention time should be set by the appliance administrator as per the retention requirement of their use case.

- Once the lockdown mode is set, only Appliance administrators can change the lockdown mode.
- The lockdown mode is maintained during upgrade.
- Only the Appliance administrator can remove the retention locks if the lockdown mode is enterprise.
- Only the users with appliance administrator role can disable retention or remove the retention lock using the MSDP Restricted Shell.
- The user cannot change the mode if any existing operation is in progress.

Restrictions in different modes

- If the mode is set to compliance mode, the administrator cannot change the mode to enterprise or normal mode.
- If lockdown mode is set to compliance or enterprise for any node, it is not available for factory reset.
- During add and replace node operations, the new node is automatically placed in the existing lockdown mode of the cluster. The lockdown mode of the node that got replaced is set to normal and the node is available for factory reset.
- Cluster maintenance shell is enabled with two-factor authentication (2FA).
- If you use the NetBackup Flex Scale UI to change the retention period without changing the lockdown mode, you have to manually update the disk volume in NetBackup, either through the NetBackup CLI or the NetBackup Web UI. This is necessary to synchronize the information in the NetBackup database.

Restricted access to Remote Management Platform (HPe iLO)

If you select enterprise or compliance mode, you can restrict remote management access to the node by selecting the **Restrict remote management access** check box. This option is not available for normal lockdown mode. Restricting remote management access to nodes provides an additional level of data security and limits the privileges and operations that you can perform.

After you enable this restriction, an IPMI Administrator user on an HPE platform has only **Login** and **Virtual Power and Reset** privileges. With these privileges, the user can only view settings in iLO and perform power-related operations.

After you enable restricted remote access, remember that:

- In enterprise lockdown mode, you can enable or disable restricted remote management access.

- In compliance lockdown mode, you can only enable restricted remote management access, but cannot disable the remote management access restriction.
- You can also choose to enable or disable restricted remote management access after the initial configuration is complete.

Warning: Once you enable restricted remote management access, all destructive operations are disabled for all the IPMI users. Users can view and perform limited operations in the IPMI web GUI but cannot access the remote console. Physical access to the system is required to logon to the console.

Table 5-2 lists the privileges given for a local account in iLO.

Table 5-2 HPE iLO

Privileges	Description
Login	Enables a user to log on to iLO.
Remote Console	Enables a user to access the host system remote console, including video, keyboard, and mouse control. Users with this privilege can access the BIOS, and therefore may be able to perform host-based BIOS, iLO, storage, and network tasks.
User Config	Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you are not assigned this privilege, you can view your own settings and change your own password.

Table 5-2 HPE iLO *(continued)*

Privileges	Description
iLO Config	Enables a user to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration. After iLO is configured, revoking this privilege from all users prevents reconfiguration from the following interfaces: ■ iLO web interface ■ iLO RESTful API ■ CLI ■ HPQLOCFG Users who have access to the following interfaces can still reconfigure iLO: ■ UEFI System Utilities ■ HPONCFG Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
Virtual Media	Enables a user to use the virtual media feature on the host system.
Virtual Power and Reset	Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.
Host NIC Config	Enables a user to configure the host NIC settings. This privilege does not affect configuration through host-based utilities.
Host Bios Config	Allows configuration of the host BIOS settings by using the UEFI System Utilities. This privilege is required for replacing the active system ROM with the redundant system ROM. This privilege does not affect configuration through host-based utilities.
Host Storage Config	Enables a user to configure the host storage settings. This privilege does not affect configuration through host-based utilities.

Table 5-2 HPE iLO *(continued)*

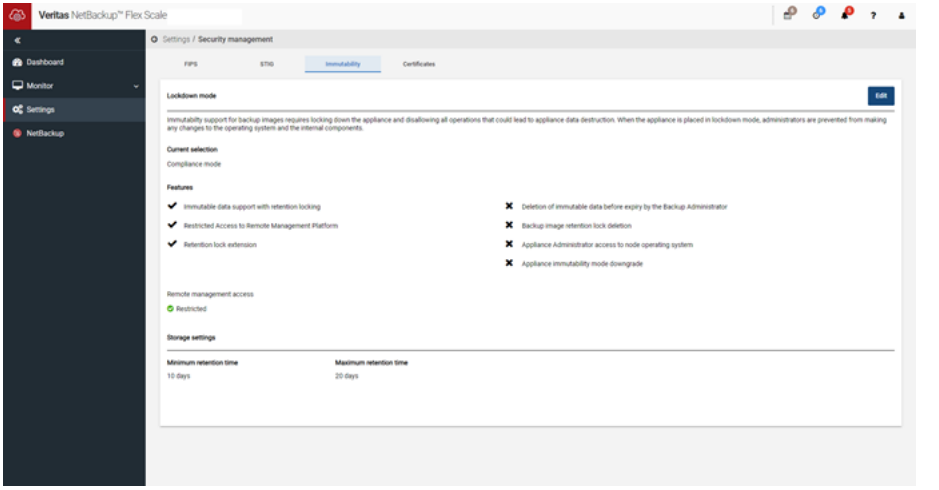
Privileges	Description
Recovery Set	Enables a user to manage the System Recovery Set. By default, the Recovery Set privilege is assigned to the default administrator account. This privilege can be added to a user account only by creating or editing the account with an account that already has this privilege. If there is no user account with the Recovery Set privilege, and an account with this privilege is required, reset the management processor to the factory default settings. The factory default reset creates a default Administrator account with the Recovery Set privilege. This privilege is not available when iLO security is disabled with the system maintenance switch. For information about the default account credentials and how to configure this privilege without access to an account that has this privilege, see the *iLO User Guide*.

Configuring immutability using GUI

You can configure immutability using the NetBackup Flex Scale GUI.

To configure immutability using GUI

1 Go to **Settings** > **Security management** > **Immutability**. Click **Edit**.



2 Choose any of the lockdown modes under **Mode Selection**. You can choose from Normal, Enterprise, and Compliance. The supported features for each mode are listed.

Note: You cannot downgrade the lockdown mode after it is configured. For example, if the lockdown mode is set to compliance, you cannot change the lockdown mode to enterprise or normal.

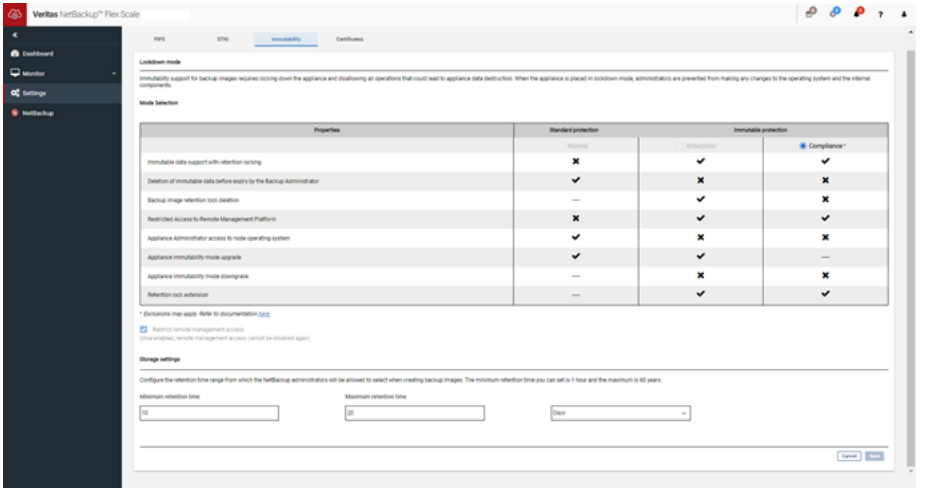
---

3 If you choose Enterprise or Compliance mode, you also have to configure the retention time range from which the NetBackup administrators will be allowed to select when creating backup images. Specify the maximum and minimum retention time. Click **Save**.

Note: Ensure that the image retention period in backup policies is within the lockdown mode retention time to avoid any error during backup.

If you select enterprise or compliance mode, you can restrict remote management access to the node by selecting the **Restrict remote management access** check box.

Warning: Once you enable restricted remote management access, all destructive operations are disabled for all the IPMI users. Users can view and perform limited operations in the IPMI web GUI but cannot access the remote console. Physical access to the system is required to logon to the console.



Authenticating users using digital certificates or smart cards

You can configure NetBackup Flex Scale to authenticate users with a smart card or a digital certificate. After configuration, the users can use the **Sign in with**

certificate or smart card option to sign in to NetBackup Flex Scale UI using smart cards or digital certificates.

Before you configure user authentication using smart cards or digital certificates, note the following:

- Digital certificate or smart card authentication can be configured for LDAP, AD, and local users.
- Ensure that LDAP is configured if you want to authenticate LDAP users by using digital certificate or smart card.
- Ensure that AD is configured if you want to authenticate AD users by using digital or smart.
- Ensure that you create a local user if you want to authenticate local users by using digital or smart card.
- Smart card authentication requires a list of trusted root or intermediate CA certificates. You must add the CA certificates that are associated with the user digital certificates or the user smart cards.

To authenticate users with a certificate or smart card for media server only deployment:

1. Use a user account with an Appliance Administrator role to log in to the NetBackup Flex Scale infrastructure management UI `https://consoleIP:14161` where *consoleIP* is the public IP address that you specified for the infrastructure management UI during the cluster configuration.
2. In the left pane click **Settings > Security > Smart card authentication**.
3. Use the slider to turn on smart card authentication.
4. In the **Configure smart card authentication** dialog box, specify the following options:
   - In the user authentication domain list, specify the following information:
     - None, which is a default option, indicates that only local users can be authenticated using smart card.
     - For an AD user, select the configured AD server.
     - For an LDAP user, select the configured LDAP server.
   - Under **Certificate mapping attribute**, to specify the user using the username format, click **Common name**. To specify the user using the username and domain format (for example, username@test.com) click **User principal name**.
   - Optionally, enter the Online Certificate Status Protocol (OCSP) URI. OSCP is used for checking the validity of the certificate. The OCSP responder is

a remote independent entity (certificate vendor authority). If you do not provide the OCSP URI, the URI in the user certificate is used.

- Click **Save**.

5 To the right of CA certificates click **Add**.

You can upload a CA certificate or a chain certificate. The leaf certificate can be created directly from root certificate or from an intermediate certificate. Chain certificate is a concatenation of root and intermediate certificate.

6 Click **Browse** to select the CA certificate or drag and drop the CA certificate and click **Add**.

Certificates must be in PEM format, with certificate file type as `.pem`. Only one certificate can be added at a time. The web server is restarted after you add the certificate and the certificate is added to the web server trust store `/shared/cluster_certs/cac/`. The selected CA certificate is displayed under CA certificates.

7 Upload the client certificate to the browser's certificate store. See the browser documentation for importing client certificates.

8 Add Appliance administrator user role to a smart card user. To add the Appliance administrator role to an AD, LDAP, or a local user, navigate to **Settings > User management**.

9 To log on using the smart card, when you enter the URL for the UI, you are prompted to select the certificate that you added to the browser trust store. Select the certificate to authenticate. Selecting the certificate is a one-time activity. You can now use the **Sign in with certificate or smart card** option to sign in to the UI.

To authenticate users with a certificate or smart card for a cluster where both the primary server and media servers are deployed:

1 Use a user account with both Appliance Administrator and NetBackup Administrator role to log in to the NetBackup Flex Scale web interface `https://`*`ManagementServerIPorFQDN`*`/webui` where *ManagementServerIPorFQDN* is the public IP address, the FQDN, or the short host name that you specified for the NetBackup Flex Scale management server during the cluster configuration.

2 At the top right, click **Settings > Smart card authentication** and follow the steps mentioned in the "Configuring authentication options" section of the *NetBackup™ Web UI Administrator's Guide*. After configuring smart card authentication, you need to perform additional steps before you can log in using a smart card.

3. Get the NetBackup Flex Scale web UI's root CA and intermediate certificates and upload it to browser:
   - Navigate to **Cluster Management > Cluster settings > Security > Certificates** and click **Download root certificate**.
   - The downloaded certificate contains two certificate keys in a single file. Separate the downloaded certificate in two files:
     - `root_ca.pem`: Upload to the browser's trusted root certificate store.
     - `stem_ca.pem`: Upload to the browser's intermediate certificate store.
4. Get NetBackup web root CA certificates and upload it to the browser. To get the NetBackup web certificate:
   - Get the NetBackup web root CA certificate using swagger or using CURL API:

     ```
     curl -X 'GET'
     \'https://primary-server-FQDN/netbackup/security/cacert' \ -H
      'accept: application/vnd.netbackup+json;version=9.0'
     ```

   - Copy the web root certificate from the received response to a file. Ensure that you replace the \n character with newline.
   - Upload the web root CA certificate to update the SAN entries in the NetBackup web certificate.
   - If you use Mozilla Firefox browser, enable **network.cors_preflight.allow_client_cert** to set it to **true**.
5. Log in to the NetBackup Flex Scale UI by clicking **Sign in with certificate or smart card** on login screen and when prompted select the certificate that you uploaded to the browser trust store.

About system certificates on NetBackup Flex Scale

NetBackup Flex Scale supports one certificate for all services. The certificate can be internal or external. The Appliance CA creates the internal certificate. Any CA can create the external certificate using a CSR generated using the NetBackup Flex Scale GUI. The CA certificate can also be downloaded using the GUI by navigating to **Settings > Security Management > Certificates**. The admin user can change the certificate mode by navigating to **Settings > Security Management > Certificates** in the GUI. After changing the certificate mode, the admin user should restart all the services to start using the new certificate.

You can navigate to **Settings > Security > Certificates > Download root certificates** to download the VxOS certificates which contain the intermediate and root CA certificates (both VxOS root and VxOS stem).

Note: Ensure that you have the latest Chrome update for the secure connection to work with VxOS certificates.

If the system certificate mode is set to internal, the certificate that is signed by the Appliance CA (internal certificate) is used for all the GUI services.

You must update the clients trust-store with CA certificate to secure connection.

Deploying external certificates on NetBackup Flex Scale

You can generate and use external certificates instead of internal certificates. External Certificate Authority (ECA) certificates are the digital credentials that attest to the certificate owner's identity and affiliation. Once you deploy the external certificates, all the NetBackup Flex Scale components use them. These include the NetBackup primary server, media server, storage engine, management gateway, and the NetBackup Flex Scale web services. One certificate is deployed for all the components. The external certificates also deploy a certificate bundle and (optionally) certificate revocation list. To generate an external certificate, you have to create a certificate request with proper 'Subject Distinguished Name' and 'Subject Alternative Names.' You can generate a certificate request using the GUI. The necessary FQDNs are auto-populated to generate the correct request. You can add additional information as needed. Based on the certificate request, you can create an external certificate. When deploying external certificate for the first time, you have to provide a CA certificate bundle. This is used to validate the incoming and deployed external certificate. You can also optionally provide a certification revocation list. NetBackup components use the CRL.

Some important terminologies:

- A certificate authority, also known as a certification authority, is a trusted organization that verifies websites (and other entities) so that you know who you are communicating with online. Their objective is to make the internet a more secure place for both organizations and users. Becoming a Certificate Authority (CA) means that you (or your customers) oversee the issuing process of cryptographic pairs of private keys and public certificates.
- Certificate bundle (CA bundle) is a file that contains root and intermediate certificates. The end-entity certificate along with a CA bundle constitutes the certificate chain.

- Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted. CRL is optional. It may be provided as a file or embedded in certificate as a URL.
- Subject Alternative Name: This field lets you specify additional host names (such as sites, IP addresses, common names) to be protected by a single SSL certificate. They are added to generate certificates for new nodes or additional VLAN IPs to be added in the future.

Considerations while deploying ECA:

- All certificates for communication should be obtained from a common trusted CA. Auto Image Replication (AIR) between MDSPs that uses different external CAs is not supported but you can concatenate the individual root CA certificates into one file and upload them as a CA bundle.
- After ECA is deployed on the cluster, you can renew or update the ECA.
- It is recommended to pause backup/restore operations before starting ECA deployment/renewal.
- The CA bundle and CRL file independent of other security artifacts.
- When you deploy security artifacts, they are validated and if inconsistencies are found, you are notified, and deployment does not proceed. If you provide an external certificate and CA certificate bundle, the EC certificate is validated against the user provided CA certificate bundle. If only one of the items is provided, it is validated against deployed artifacts.
- Only NetBackup Certificate Authority (NBCA) + ECA deployment is supported in this release.
- You cannot revert to NBCA deployment once NBCA + ECA deployment is done.
- You do not get any alert for NBCA expiry or renewal. An event is raised when NBCA is about to expire and renewed in the background.
- NBCA is auto renewed 60 days before expiration.
  If NBCA renewal fails, a failed task can be seen on NetBackup Flex Scale GUI.
- You are notified 60 days before the expiration of the ECA certificates. An alert appears on the appliance GUI and an email is also sent.
- You can deploy external certificate only if all NetBackup Flex Scale components are up and running. These include NetBackup primary and media services, storage engines, management gateway, and NetBackup Flex Scale management web services.
- You cannot deploy security artifacts, if upgrade, add node or VLAN operation is in progress and vice versa.

- If the ECA's subject alternative names have information on new nodes (FQDNs) to be added, add node operation succeeds seamlessly and all services come up after the add node operation. If subject alternative names are not updated, add node operation fails.
- For Nutanix, HBase workloads using SSL certificates, append the respective SSL certificates to the CA bundle after ECA certificates are renewed. If you do not append the SSL certificates to the CA bundle during ECA renewal, backup and restore operations for the workloads may fail.
- If you want to deploy ECA on a cluster on which disaster recovery is already configured, ensure that you configure ECA on the primary cluster.
- If ECA is deployed on the primary cluster before adding the secondary cluster, then you must redeploy ECA from the primary cluster after disaster recovery configuration is complete. This is to ensure proper connectivity between the primary server, media server, and storage services.
- If CRL mode is selected as CRL URL during ECA deployment, ensure that the CRL URL host name is resolvable by the existing DNS servers. If there are no DNS servers or if the DNS server cannot resolve the CRL URL host name, you must add the CRL URL as a custom host entry for the NetBackup container and the cluster nodes. This is also applicable if a DNS server is present during ECA deployment but is removed later.
- If you do not want to generate CSR from the GUI, then you can use your own certificate for ECA deployment. In such a scenario, you must upload your own unencrypted private key.
- If ECA is configured with the CRL as an URL, and if the CRL server becomes unreachable or unavailable for more than 24 hours for any reason, the NetBackup services on the NetBackup Flex Scale cluster appears as degraded. Once the connectivity to the CRL server is established again, the NetBackup services appear as healthy.

Considerations while deploying ECA on a cluster on which only media server is deployed:

There are some additional considerations that you need to keep in mind when you deploy ECA on a media server only cluster.

- If you have deployed media server only clusters with external NetBackup primary server on BYO:

  If ECA deployment is done after media server only configuration:

  - The primary server should be configured in ECA + NBCA mode before starting ECA deployment on the cluster.

- The CA chain (Root + Intermediate) used should be same trusted certificate chain for both primary and media server only cluster.

If media server only deployment is done after ECA configuration on NetBackup BYO:

- Pure ECA mode is not supported.
- If the primary server is deployed in NBCA + ECA mode then media server can be deployed using it and ECA can be configured on media server only cluster.
- The CA chain (Root + Intermediate) used should be same trusted certificate chain for both primary and media server only cluster.

- If you have deployed media server only cluster with external NetBackup primary server in a NetBackup Flex Scale cluster:

  If ECA deployment is done after media server only configuration:

  - Primary server should be configured in ECA + NBCA mode before starting ECA deployment on the media server only cluster.
  - This can be done using the NetBackup Flex Scale ECA deployment workflow.
  - The CA chain (Root + Intermediate) used should be same trusted certificate chain for the cluster on which both primary and media servers are deployed and media server only cluster.

  If media server only deployment is done after ECA configuration on a NetBackup Flex Scale cluster on which both primary and media server are deployed

  - Pure ECA mode is not supported a NetBackup Flex Scale cluster on which both primary and media server are deployed.
  - If the cluster is deployed in NBCA +ECA mode, then media server only cluster can be deployed using it and ECA can be configured on media server only cluster.
  - The CA chain (Root + Intermediate) used should be same trusted certificate chain for the cluster on which both primary and media servers are deployed and media server only cluster.

Deploying ECA using the GUI

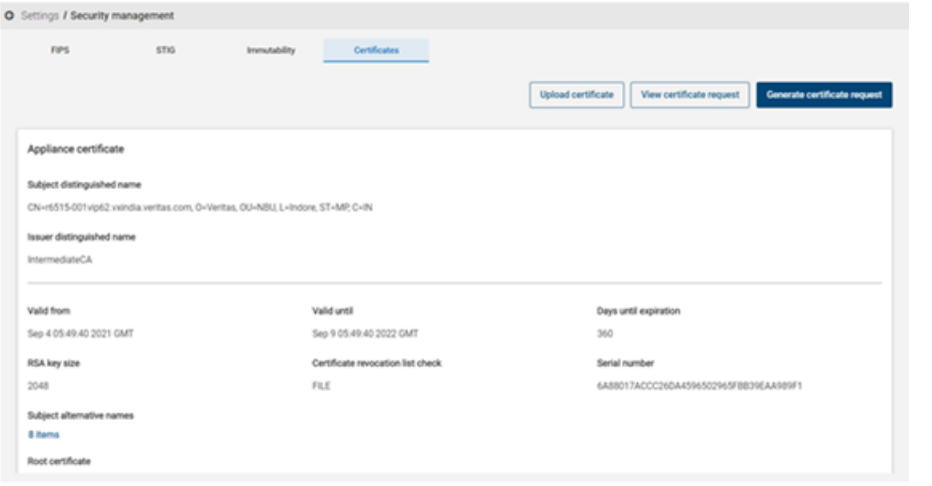
You can perform all external certificates related operations from the **Settings** > **Security Management** > **Certificates** tab.

- Upload certificate
- View certificate request

- Generate certificate request

To deploy ECA using the GUI

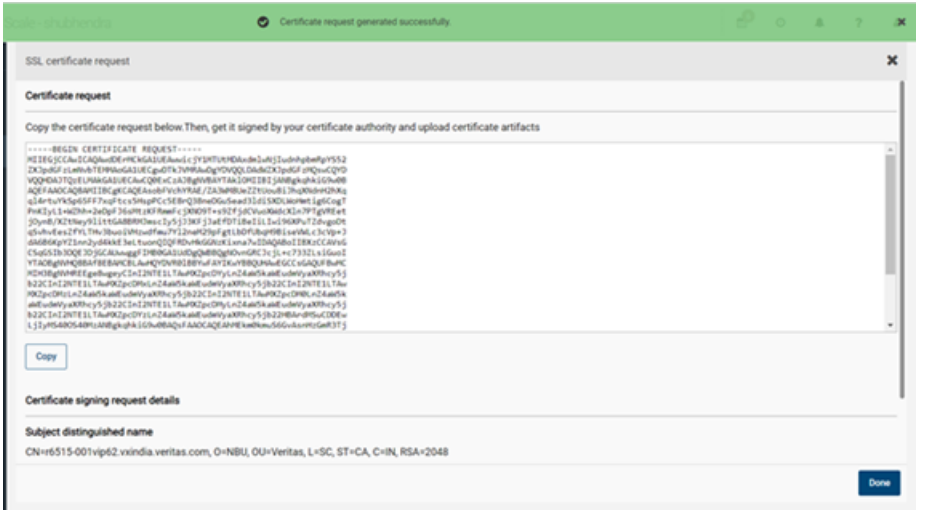
1. Go to the **Settings** > **Security Management** > **Certificates** tab.
2. Click **Generate certificate request** and fill out the form. The SAN field is filled with default SAN entries that are mandatory for the configuration. For standard default configuration, it has the FQDN entries for all the storage servers, NetBackup primary FQDN, console IP and API gateway FQDN.



3 Click **Generate** to generate a certificate request.

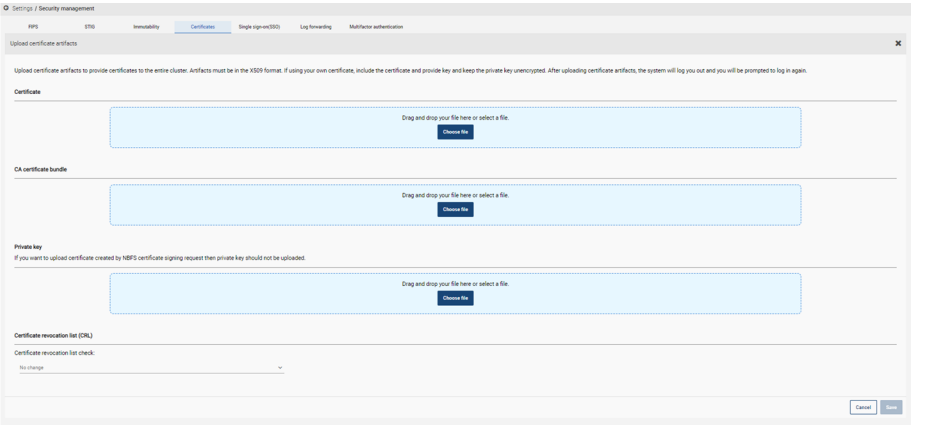
The CSR is used to generate certificate. This certificate along with the CA bundle (Root CA + Intermediate CA) should be uploaded on the upload page.

4 Click **Copy** to copy the certificate request. This has to be given to a CA signing authority who uses this to generate a certificate. CA signing authority will provide a certificate along with the root certificate and intermediate certificate used to generate the certificate. Authority may also provide a CRL file.



5 Go to **Certificates** > **Upload certificate** to upload the certificate artifacts. For a fresh deployment, both the certificate and CA certificate bundle are mandatory. CRL is optional. For renewal, any one of the three are required.

Both the certificate and CA bundle must be a .PEM file. The CA bundle .PEM file should contain entries for all the CA certificates from root to intermediate till the immediate parent of the leaf certificate.



6 After the certificate is uploaded, **Save** gets enabled. Click **Save**. The deployment is initiated.

After deployment is successfully completed for all components, the GUI restarts with the uploaded external certificate.

You can verify the browser certificate from the GUI to verify that it is the same one that was used during deployment.

Log locations

The configuration file can be found at location: `/shared/security_artifacts/config.json`. It contains information about CSR, current key size, and whether ECA is deployed and the details of the nodes on which it is deployed.

The deployed artifacts can be found at the location: `/shared/security_artifacts/`.

All the logs pertaining to ECA deployment are present in the `/log/VRTSnas` directory:

- nbfs_deploy_certificate.log: It contains the logs of the driver script which is responsible for performing pre-checks and then calling subsequent scripts to deploy ECA on various components.

- ec_validate.log: It contains the logs for the ec_validate script responsible for performing validations on the artifacts.
- nbu_nbca_certificate_deploy.log: It contains the logs for the NBCA deployment on NetBackup components.
- nbu_eca_certificate_deploy.log: It contains the logs for ECA deployment for NetBackup components.
- isagui_deploy_mgmt_cert.log: It contains the logs for deployment of ECA on NetBackup Flex Scale GUI and API gateway.
- nbfs_deploy_cert_on_node.log: It contains the logs when ECA is internally deployed on newly added or replaced node in add/replace node workflow if ECA is already deployed.

Considerations for performing other operations when ECA is deployed

If ECA is deployed and you want to add a new node to the cluster:

- Before starting an add node operation, generate a new certificate request which has the new node's storage server FQDN as an additional SAN entry.
- Do not add the media server FQDN in the SAN entry.
- Upload the new certificate and then add the new node. Otherwise, the add node operation will fail.

If ECA is deployed on a cluster where disaster recovery is configured and you want to add a new node to the cluster:

- The ECA has to be renewed on the primary irrespective of whether you add the new node on the primary or secondary cluster.
- The new certificate must contain FQDN of the storage server of the node which is going to be added.
- A new CSR has to be generated which contains the FQDN of the new storage server as a SAN entry. A new certificate is generated with the new CSR which is used for ECA deployment/renewal.
- Do not add the media server FQDN in the SAN entry.

If ECA is deployed and you want to add a new data network:

- Add the new primary and storage server FQDNs to the CSR and deploy the new certificate before adding the new data network.
- Do not add the media server FQDN in the SAN entry.

About multifactor authentication

Multifactor authentication is a robust security measure widely used for adding an additional layer of security to the authentication process by requiring users to provide a unique, time-limited code along with their regular login credentials. It is a multiple-step account login process that requires you to enter a 6-digit one-time password along with your password.

It is strongly recommended that you configure multifactor authentication to protect the security of your account.

See "Configuring multifactor authentication for your user account" on page 246.

If multifactor authentication is enforced in the NetBackup Flex Scale cluster, all users must configure multifactor authentication for their user accounts for successful sign-in.

See "Configuring multifactor authentication for your user account when it is enforced in the cluster" on page 248.

Considerations before configuring multifactor authentication

Some considerations that you need to remember before you configure multifactor authentication:

- The Appliance administrator can see the status of all the users on the **Settings > User management** page.
- If AD/LDAP server configuration is removed from the cluster without removing the AD/LDAP user's MFA configuration, the Appliance administrator may see stale entries for AD/LDAP users.
- If you are an AD/LDAP user with no role, you cannot login to the appliance.
- A local administrator is a non AD/LDAP user.
- If NetBackup Flex Scale has been deployed with both primary and media servers, and if the user does not have the Appliance administrator role and has only NetBackup administrator role, the user is directed to the home screen.
- Local administrator users' roles must be assigned from the NetBackup Flex Scale GUI.
- When catalog replication for disaster recovery is configured between two NetBackup FlexScale clusters, users are managed independently on each cluster and the corresponding multifactor authentication configuration should be done separately on each cluster. Veritas recommends that you use the following guidelines when making user configuration changes in a NetBackup Flex Scale cluster on which disaster recovery is configured:

- When adding local users, both the clusters should use the same credentials.
- AD/LDAP configuration must be performed only on the primary cluster on which disaster recovery is configured.
- When configuring multifactor authentication for a user, the same multifactor authentication secret key must be used for both clusters.
- When enforcing multifactor authentication, it should be enforced with the same start date on both the clusters.

Configuring multifactor authentication for your user account

You must first install and configure authenticator application on your smart device that provides you with the one-time password.

Supported authenticator applications

If the NetBackup Flex Scale administrator has enforced multifactor authentication in the NetBackup Flex Scale cluster, you must configure it for your user account for successful sign-in. You must configure multifactor authentication before the start date of enforcement. Else, you will lose access to the appliance and your automation workflow (if using login API) will also be impacted.

Even if multifactor authentication is not enforced, it is recommended that you configure it for enhanced security.

To configure multifactor authentication for your user account

1. Sign in to the NetBackup Flex Scale UI.
2. On the top right, click the profile icon and click **Manage multifactor authentication**.
3. On the **Manage multifactor authentication** screen, click **Configure**.
4. On the next screen, follow the given steps.

   Install and configure authenticator application on your smart device. It generates one-time password and sends it on your smart device.
5. Scan the QR code with the authenticator application or enter the key manually.

   The manual key should be base32 encoded and can contain between 26 to 208 characters with or without padding.
6. Enter the one-time password that you see in the authenticator application.
7. Click **Configure**.

   At the time of next sign-in, you need to enter the one-time password along with the username and password.

See “Disabling multifactor authentication for your user account” on page 247.

Disabling multifactor authentication for your user account

You can disable MFA for your user account only If multifactor authentication is not enforced. However, it is strongly recommended that you configure multifactor authentication to protect the security of your account.

If multifactor authentication is enforced, and you want to reset it, See “Resetting multifactor authentication for a user” on page 249.

To disable multifactor authentication for your user account

1. Sign in to the NetBackup Flex Scale UI.
2. If you are an Appliance administrator, click the profile icon on the top right, and select **Manage multifactor authentication**.

   If you are not an Appliance administrator, select **Manage multifactor authentication** in the home screen.
3. If you have already configured multifactor authentication for your user account, you can see the **Disable** button.
4. Click **Disable**.
5. Enter the one-time password and click **Submit**.

Enforcing multifactor authentication for all users

Only the NetBackup Flex Scale administrator can enforce multifactor authentication for all NetBackup Flex Scale users.

Before you enforce multifactor authentication:

- Multifactor authentication can be enforced only if at least two local users have configured it.
- You can set a future start date for enforcement so that the users get sufficient time to configure their multifactor authentication.
- If multifactor authentication is not configured by the start date, the user will not have access to the appliance. If the user's automation workflow uses login API, then that will also be impacted.
- Once multifactor authentication is enforced, it cannot be reversed.
- It is not possible to postpone the start date of enforcement after it is set.
- You can prepone the start date for enforcement using the **Reinforce** button on the **Settings > Security management > Multifactor authentication** page.

- The start date for enforcement cannot be more than 90 days from the current date.

To enforce multifactor authentication for all users

1. Sign in to the NetBackup Flex Scale UI.
2. Go to **Settings > Security management > Multifactor authentication**.
3. Click **Enforce** to enforce multifactor authentication for all NetBackup Flex Scale users.

   Notify all users that they must configure multifactor authentication for their user accounts to be able to successfully sign in.

   See "Configuring multifactor authentication for your user account" on page 246.

Configuring multifactor authentication for your user account when it is enforced in the cluster

After multifactor authentication is enforced in the cluster, you must configure it for your user account if you have not already configured it. If you do not configure multifactor authentication for your account after the enforcement, you cannot sign-in to the appliance and any automation workflow using the login API will also be impacted.

To configure multifactor authentication after the enforcement

1. Open a web browser and go to the following URL.

   https://*console-IP*:14161/login

   The *console-IP* is the management console IP address where the web interface is hosted.
2. Enter the **Username** and **Password**.
3. Click **Sign in**. The **Configure multifactor authentication** screen is displayed.
4. On the next screen, follow the given steps.

   Install and configure an authenticator application on your smart device. It generates a one-time password and sends it to your smart device.

   Supported authenticator applications
5. Scan the QR code with the authenticator application or enter the key manually.

   The manual key should be base32 encoded and can contain between 26 to 208 characters with or without padding.

6 Enter the one-time password that you see in the authenticator application.

7 Click **Submit**.

Successful configuration takes you back to the sign-in screen.

Enter the username, password, and one-time password for successful sign-in.

Resetting multifactor authentication for a user

Only the NetBackup Flex Scale administrator can reset multifactor authentication for other NetBackup Flex Scale users.

Before you reset multifactor authentication:

- The logged in administrator cannot reset his own multifactor authentication. It can only be reset by another Appliance administrator.
- If multifactor authentication is not enforced, then it is possible to reset it for any user.
- If multifactor authentication is enforced, then you can reset it for a local (non AD/LDAP) administrator only if at least one other local administrator is present who has multifactor authentication configured.

To reset multifactor authentication for an NetBackup Flex Scale user

1 Sign in to the NetBackup Flex Scale UI.

2 Go to **Settings > User management**.

3 Navigate to the user row and click on the vertical ellipsis button from the right side of the UI and then select **Reset multifactor authentication** .

4 In the **Reset multifactor authentication** pop-up, click **Reset**.

About single sign-on (SSO) configuration

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Cohesity product.

Note the following requirements and limitations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Configuration of the IDP requires the NetBackup Flex Scale GUI.
- Global logout is not supported.

Configuring SSO on a NetBackup Flex Scale cluster on which both primary and media servers are deployed

Configuring SSO on NetBackup Flex Scale cluster on which both primary and media servers are deployed involves the following steps:

Table 5-3

Task	Description
Configuring SSO on an NetBackup Flex Scale cluster	See To configure SSO on a cluster on which both primary and media servers are deployed
Adding users/group	See To add users/group in RBAC
Configuring an identity provider	See To configure an identity provider
Logging into NetBackup Flex Scale with SSO	See Login with SSO

Configuring SSO on an NetBackup Flex Scale cluster

To configure SSO on a cluster on which both primary and media servers are deployed

1. Go to **Settings > Security management > Single sign-on (SSO)**. Click **Add**.
2. Give the IDP name and upload the IDP metadata xml and optionally provide the custom user field and group field values. The user field and group field values should be same as configured on the IDP. Click **Save**.

   The UI displays a message that confirms that the add identity provider task is triggered. You can click **View Details** to see the progress of the task. Alternatively, you can also click the **Recent Activity** icon from the top right of the UI to see the status of the most recent operations.
3. Once the configuration is complete, the SSO identify provider details are displayed on the screen. Click **Download service provider xml** to download the details and upload it on IDP server, if required.

Adding users/group in RBAC

To add users/group in RBAC

1. Login to the NetBackup web UI. Go to **Security > RBAC**.
2. Select the Appliance Administrator role and select the **Users** tab.
3. Add the user/group name with domain and select the user as SAML user or SAML group. Click **Add to list**.

Configuring an identity provider

To configure an identity provider

- Login with SSO works only if the configuration on the IDP side is done. Each IDP has different steps for configuration.

  Refer to the following links for the configuration steps for each identity provider.

  - ADFS: Enrolling NetBackup Flex Scale primary server as a service provider to ADFS
  - Azure: Enrolling NetBackup Flex Scale primary server as a service provider to Azure
  - Okta: Enrolling NetBackup Flex Scale primary server as a service provider to Okta
  - PingFederate: Enrolling NetBackup Flex Scale primary server as a service provider to PingFederate

Logging into NetBackup Flex Scale with SSO

Login with SSO

1. Navigate to infrastructure GUI login page. Click **Sign-in with single sign-on (SSO)**.
2. Enter SSO credentials and click **Sign in**.

Limitations

There are some limitations when you configure SSO on a NetBackup Flex Scale cluster on which both primary and media servers are deployed.

- Identity provider cannot be edited. It can be removed and added again.
- If the same identity provider is removed and added again with a different name, then all the existing SAML users for that IDP will not be able to login. In such cases, either the admin has to remove and add the SAML users and groups in RBAC again or keep the same name when adding the identity provider.
- Single logout is not implemented. If SAML users log out of the application, and try to login with SSO again, the user is not asked for their login credentials unless the SSO session has expired. This applies to any other application using the same IDP.
- If after identity provider configuration, External certificate authority (ECA) is configured, then login with SSO does not work until the identity provider is updated with the latest service provider metadata xml from the NetBackup Flex Scale. This can be done by downloading the service provider metadata xml from

Settings > Security > Single-Sign on > Download service provider metadata. This metadata needs to be updated on the IDP side.

- AD/IDP server date, time, and time zone should be the same as the NetBackup Flex Scale cluster. Else, the SSO login fails.
- SAML users or the SAML group users cannot login using the NetBackup Flex Scale login screen for a cluster on which both primary and media servers are deployed.
- SAML users or SAML group users cannot configure multifactor authentication option available in the **Security > Multifactor authentication** section.
- If disaster recovery or primary service replication is configured after the SSO is configured on both the primary and secondary clusters, then the identity provider configured on the secondary cluster ceases to exist and the SAML users in its RBAC cannot login using SSO. Only the primary cluster SAML users can login using SSO on both the clusters.
- If disaster recovery or primary service replication is configured after the SSO is configured on only the secondary cluster, then SSO is unconfigured as its NetBackup primary cluster points to the primary cluster.
- If SSO is configured after disaster recovery configuration from either the primary or secondary cluster, then it is configured for both the clusters and users can login with SSO for both clusters.

Log location

The logs can be found by logging into the NetBackup Flex Scale CLISH, elevating to root and accessing the logs at:

- `/log/VRTSnas/ nbu_sso_config.log`
- `/log/VRTSnas/ isagui_webserver.log`
- `/log/VRTSnas/ isagui_sso_config.log`

The Table 5-4 lists the common error messages.

Table 5-4 Common error messages

Error message	Description
`You are not authorized to access this application`	User is a valid AD/LDAP and IDP user but does not have the Appliance administrator role in NBU RBAC or the Identity provider was deleted and added again with a different name after adding the SAML users in NetBackup RBAC.

Table 5-4 Common error messages *(continued)*

Error message	Description
`Authentication failed, userPrincipalName field not found in response`	SAML response from the IDP does not contain the user field. This can be due to userPrincipalName field attribute mapping not being created on the IDP side or the custom attribute name is different on the IDP side as provided in the NetBackup Flex Scale.
`Unable to get response from identity provider`	Date and time of Identity provider does not match with NetBackup Flex Scale cluster, Identity provider certificate is not updated with latest NetBackup primary certificate, or the certificate revocation check is not disabled on the identity provider.

Configuring SSO on a NetBackup Flex Scale cluster on which only media servers are deployed

Configuring SSO on NetBackup Flex Scale cluster on which only media servers are deployed involves the following steps:

Table 5-5

Task	Description
Configuring SSO on an NetBackup Flex Scale cluster	See To configure SSO on cluster on which only media servers are deployed
Adding users/group	**Note:** SSO can be configured only for AD/LDAP users for media server only deployment.
Configuring an identity provider	See To configure an identity provider
Logging into NetBackup Flex Scale with SSO	See Login with SSO

Configuring SSO on an NetBackup Flex Scale cluster

To configure SSO on cluster on which only media servers are deployed

1. Go to **Settings > Security management > Single sign-on (SSO)**. Click **Add**.
2. Give the IDP name and upload the IDP metadata xml and optionally provide the custom user field and group field values. The user field and group field values should be same as configured on the IDP. Click **Save**.

   The UI displays a message that confirms that the add identity provider task is triggered. You can click **View Details** to see the progress of the task. Alternatively, you can also click the **Recent Activity** icon from the top right of the UI to see the status of the most recent operations.
3. Once the configuration is complete, the SSO identify provider details are displayed on the screen. Click **Download service provider xml** to download the details and upload it on IDP server, if required.

Configuring an identity provider

To configure an identity provider

- Login with SSO works only if the configuration on the IDP side is done. Each IDP has different steps for configuration.

  Refer to the following links for the configuration steps for each identity provider.

  - ADFS: Enrolling NetBackup Flex Scale primary server as a service provider to ADFS
  - Azure: Enrolling NetBackup Flex Scale primary server as a service provider to Azure
  - Okta: Enrolling NetBackup Flex Scale primary server as a service provider to Okta
  - PingFederate: Enrolling NetBackup Flex Scale primary server as a service provider to PingFederate

Logging into NetBackup Flex Scale with SSO

Login with SSO

1. Navigate to infrastructure GUI login page. Click **Sign-in with single sign-on (SSO)**.
2. Enter SSO credentials and click **Sign in**.

Limitations

There are some limitations when you configure SSO on a NetBackup Flex Scale cluster on which only media servers are deployed.

- Identity provider cannot be edited. It can be removed and added again.
- Single logout is not implemented. If SAML users log out of the application, and try to login with SSO again, the user is not asked for their login credentials unless the SSO session has expired. This applies to any other application using the same IDP.
- If after identity provider configuration, External certificate authority (ECA) is configured, then login with SSO does not work until the identity provider is updated with the latest service provider metadata xml from the NetBackup Flex Scale. This can be done by downloading the service provider metadata xml from **Settings > Security > Single-Sign on > Download service provider metadata**. This metadata needs to be updated on the IDP side.
- AD/IDP server date, time, and time zone should be the same as the NetBackup Flex Scale cluster. Else, the SSO login fails.

Log location

The logs can be found by logging into the NetBackup Flex Scale CLISH, elevating to root and accessing the logs at:

- `/log/VRTSnas/ nbu_sso_config.log`
- `/log/VRTSnas/ isagui_webserver.log`
- `/log/VRTSnas/ isagui_sso_config.log`

The Table 5-6 lists the common error messages.

Table 5-6 Common error messages

Error message	Description
`User is not authorized`	User is a valid AD/LDAP and IDP user but does not have the Appliance administrator role in NetBackup Flex Scale user management.
`User principal name missing/ Failed to get user details from identity provider`	SAML response from the IDP does not contain the user field. This can be due to userPrincipalName field attribute mapping not being created on the IDP side or the custom attribute name is different on the IDP side as provided in the NetBackup Flex Scale.

Table 5-6 Common error messages *(continued)*

Error message	Description
`Authentication Failed, Invalid document signature`	Date and time of Identity provider does not match with NetBackup Flex Scale cluster, Identity provider certificate is not updated with latest NetBackup primary certificate, or the certificate revocation check is not disabled on the identity provider.
`Authentication Failed, SAML assertion is not yet valid`	Date and time of Identity provider do not match with NetBackup Flex Scale cluster.
`Single sign-on failed due to an internal error`	Processing SAML callback response failed on NetBackup Flex Scale side due to some exception.

Configuring isolated recovery environment (IRE)

Organizations can minimize ransom demands by using encryption and creating a stringent security perimeter. In addition, they need to isolate, analyze, and preserve a copy of data to ensure business continuity. IRE enables organizations to meet these needs and satisfy strict regulatory and retention requirements. Veritas customers can easily deploy an IRE using their existing Veritas NetBackup infrastructure as part of a multi-layered resiliency strategy.

NetBackup Flex Scale uses the Pull model to pull the replication request from the IRE domain through a specific window as defined in the IRE air gap schedule. By initiating a data transfer request from inside the IRE domain, there is better control over data flow to secure the environment further both logically and physically. You can determine the Service Lifecycle Policy (SLP) windows and configure the air-gapped schedule for maximum protection.

The NetBackup Flex Scale IRE solution optimizes data movement whereby the request to send data comes from the IRE side, the MSDP reverse connection. You can deploy another the tertiary copy of the backup images behind a firewall to an isolated environment without opening any inbound firewall ports to NetBackup. This keeps the environment secure, allowing a sandbox approach to perform malware scans or test recovery procedures before recovering at a larger scale. You can optionally add a physical air gap as an additional layer of protection. By empowering the destination environment to request the data from the source environment (by invitation only), it is possible to support 24x7 data movement while isolating the stored data from any potential threats.

The IRE solution also supports multiple configurations. Hence, you can have a single IRE domain for multiple production domains. Another key feature of this solution is that the IRE domain is not required to have the same configuration as your production domain. You can configure an IRE domain as per your requirements and use it to securely transfer backups from production to IRE.

The requirements to configure isolated recovery environment (IRE) in a Pull model are as follows:

- NetBackup Flex scale Appliance: 3.2 or later
- Storage server: 19.0.1 or later
- NetBackup: 10.3.0.1 or later

For more information, refer to the NetBackup Deduplication Guide on SORT.

Chapter 6

Steps to protect Access Appliance

This chapter includes the following topics:

About Access Appliance hardening

This chapter contains information on the Access Appliance features that can help to secure your data protection infrastructure. For more detailed information about Access Appliance security, see the *Veritas Access Appliance Administrator's Guide*.

FIPS 140-2 conformance for Access Appliance

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for validating cryptography modules. The FIPS 140-2 standard specifies the security requirements for cryptographic modules and applies to both the hardware and the software components. It also describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

For more information about the FIPS 140-2 standard and its validation program, see the following links:

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

Starting with Access Appliance 7.4.3, FIPS 140-2 standard is enabled by default for the Veritas Operating System (VxOS). The FIPS mode for VxOS is enabled with the default factory settings. After FIPS for VxOS is enabled, the `sshd` uses the following FIPS approved ciphers:

- aes128-ctr
- aes192-ctr
- aes256-ctr

Older SSH clients are likely to prevent access to the appliance after FIPS for VxOS is enabled. Ensure that your SSH client supports the listed ciphers, and upgrade to the latest version if necessary. Default cipher settings are not typically FIPS-compliant, which means you might need to select them manually in your SSH client configuration.

Starting with Access Appliance version 8.2, the application layer is FIPS-compliant.

You can enable the FIPS 140-2 standard for NetBackup MSDP to increase appliance security. See “Enabling FIPS for Access Appliance” on page 260.

Viewing FIPS status for Access Appliance

The Federal Information Processing Standards (FIPS) 140-2 standard is enabled for Veritas Operating system (VxOS) with the default factory settings. You can view the FIPS status of VxOS for a cluster node and the FIPS status of NetBackup MSDP for each Veritas Data Deduplication server configured for the cluster.

To view the FIPS status:

1. Log in to the Access Appliance web interface of the configured cluster by opening a supported browser and typing:

   http://*console-ip*:14161

   where *console-ip* is the management console IP address where the web interface is hosted.

2. In the navigation pane, click **Settings**, and then click **Security management**.

   On the **FIPS** tab, the VxOS FIPS status for both the cluster nodes and the MSDP FIPS status for each Veritas Data Deduplication server configured for the cluster is displayed:

   - **Enabled**: The FIPS mode is enabled.
   - **Disabled**: The FIPS mode is disabled.
   - **Unknown**: The FIPS status cannot be retrieved because the Veritas Data Deduplication server is stopped, shut down, or unreachable.

Enabling FIPS for Access Appliance

You can enable the FIPS mode for NetBackup MSDP for each Veritas Data Deduplication server that is configured for the cluster. A maximum of two Veritas Data Deduplication servers can be configured.

When you enable FIPS for MSDP, all backup and restore jobs that are in progress are terminated. After you enable the FIPS mode, restart the NetBackup services to restart the jobs.

To enable the FIPS mode for NetBackup MSDP, complete the following steps:

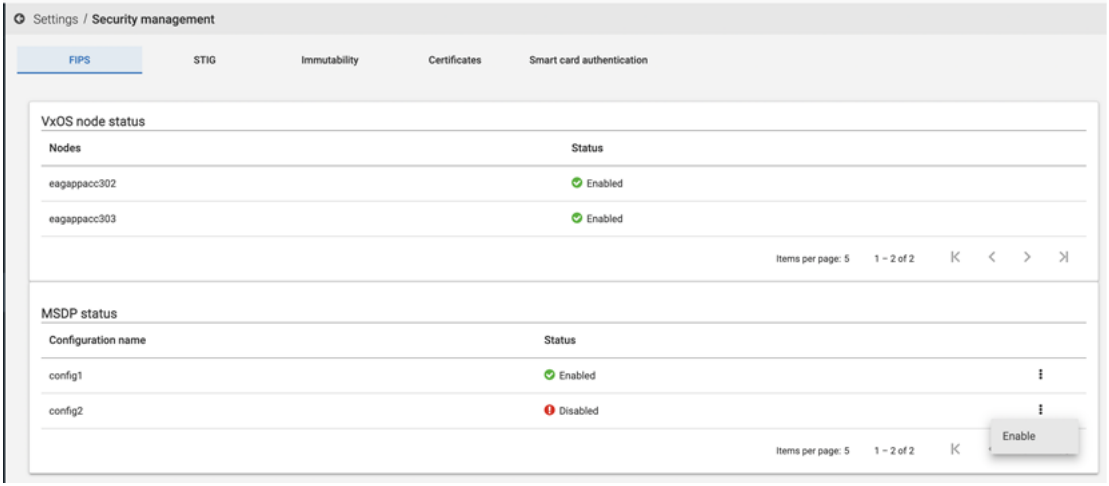
1. Log in to the Access Appliance web interface of the configured cluster by opening a supported browser and typing:

   http://*console-ip*:14161

   where *console-ip* is the management console IP address where the web interface is hosted.

2. In the navigation pane, click **Settings**, and then click **Security management**.

3 On the **FIPS** tab under **MSDP status**, for the Veritas Data Deduplication server for which you want to enable the FIPS mode click the Actions menu (three vertical dots), and then click **Enable**.



4 Review the compatibility list to ensure that all components that communicate with the FIPS service are FIPS compliant. Confirm that you have reviewed the compatibility list and click **Continue**.

5 To monitor the progress, click **View details** on the **Security** page. The ongoing and completed tasks for the operation are also displayed in **Recent activity**.

After the operation is complete, you can view the FIPS status for the Veritas Data Deduplication servers configured for the cluster:

- **Enabled**: The FIPS mode is enabled for the Veritas Data Deduplication server.
- **Disabled**: The FIPS mode is disabled for the Veritas Data Deduplication server.
- **Unknown**: The FIPS status cannot be retrieved because the Veritas Data Deduplication server is stopped, shut down, or unreachable.
  You can enable the FIPS mode again if the status is set to **Unknown** .

Disabling FIPS mode for NetBackup MSDP

You can disable the FIPS mode for NetBackup MSDP for each Veritas Data Deduplication server that is configured for the cluster. A maximum of two Veritas Data Deduplication servers can be configured for the cluster.

To disable the FIPS mode for NetBackup MSDP, complete the following steps:

1. Log in to the Access Appliance web interface of the configured cluster by opening a supported browser and typing:

   `http://`*`console-ip`*`:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.
2. In the navigation pane, click **Settings**, and then click **Security management**.
3. On the **FIPS** tab under MSDP status, for the Veritas Data Deduplication server for which you want to enable the FIPS mode click the Actions menu (three vertical dots), and then click **Disable**.
4. To monitor the progress, click **View details** on the **Security** page. The ongoing and completed tasks for the operation are also displayed in **Recent activity**.

Managing the FIPS mode using the command-line interface

You can view the FIPS status and enable and disable the FIPS mode from the Access command-line interface.

Viewing FIPS status for the appliance

You can view the VxOS FIPS status for a cluster node and the FIPS status of NetBackup MSDP for each Veritas Data Deduplication server that is configured for the cluster.

To view the FIPS mode for VxOS and MSDP:

1. Log in to the Access command-line interface as an administrator by opening an SSH session to the console IP.
2. In the Access command-line interface, run the following command:

   ```
   system security fips show
   ```

Enabling FIPS mode

You can enable the FIPS mode for NetBackup MSDP for each Veritas Data Deduplication server that is configured for the cluster. A maximum of two Veritas Data Deduplication servers can be configured. When you enable FIPS for MSDP, all the backup and restore jobs that are in progress are terminated. After you enable the FIPS mode, restart the NetBackup services to restart the jobs.

To enable FIPS for MSDP:

1. Log in to the Access command-line interface as an administrator by opening an SSH session to the console IP.
2. In the Access command-line interface, run the following command:

   ```
   system security fips enable MSDP [config_name]
   ```

   config_name is the name of the deduplication server and is optional if only one deduplication server is configured for the cluster. By default the parameter value is set to **vxdefault**.

Disabling FIPS for MSDP:

1. Log on to the Access command-line interface as an administrator by opening an SSH session to the console IP.
2. In the Access command-line interface, run the following command:

   ```
   system security fips disable MSDP [config_name]
   ```

   config_name is the name of the deduplication server and is optional if only one deduplication server is configured for the cluster. By default the parameter value is set to **vxdefault**.

Managing the login banner using the UI

You can create a customized text banner that appears when you sign in to Access Appliance UI or the system console. You can use the login banner to communicate various kinds of messages to users. Typical uses for the login banner include legal notices, warning messages, and company policy information.

If the Security Technical Implementation Guide (STIG) mode is enabled for the cluster, the login banner cannot be modified.

To set the login banner:

1. Log in to the web interface of a configured Access Appliance cluster by opening a supported browser and typing:

   ```
   http://console-ip:14161
   ```

   where *console-ip* is the management console IP address where the web interface is hosted.
2. In the left navigation pane, click **Settings** and then click **User management**.
3. Click **Manage sign-in banner**.

   If a banner is already set, the Manage sign-in banner page displays the current banner.

4. On the Manage sign-in banner page, click **Edit**.
5. (Optional) Under **Sign-in banner heading**, enter the banner heading. The heading can be a maximum of 250 characters.
6. Under **Sign in banner text**, enter the text for the banner message. The message can be a maximum of 4000 characters.
7. To review the changes, click **Preview**.
8. To confirm the changes, click **Save**.

Managing the banner from the command-line interface

You can create a customized text banner that appears when you sign in to Access Appliance UI or the system console. You can use the login banner to communicate various kinds of messages to users. Typical uses for the login banner include legal notices, warning messages, and company policy information.

If the Security Technical Implementation Guide (STIG) mode is enabled for the cluster, the login banner cannot be modified.

To display the banner:

1. Log on to the Access command-line interface by opening an SSH session to the management console IP as an administrator.
2. In the Access command-line interface, run the following command:

```
system banner get
```

```
access-clus> system banner get
No login banner is currently set for the appliance.
```

Note: No banner is set by default.

To set the banner:

1. Log on to the Access command-line interface by opening an SSH session to the management console IP as an administrator.
2. In the Access command-line interface run the following command:

```
system banner get
```

```
# access-clus> system banner set
Enter Header (Type <enter> and <Ctrl + d> to complete the body. Max 250
characters)
This is header
Enter Body (Type <enter> and <Ctrl + d> to complete the body. Max 4000
characters)
This is body text line 1.
This is body text line 2.
```

The banner is made up of two parts, the header and the body. The header is the heading for the banner and the body is the banner content. The header can be a maximum of 250 characters and body can be a maximum of 4000 characters.

After the banner is set, you can view the banner using the `system banner get` command:

```
access-clus> system banner get
****************
 This is header
****************
This is body text line 1.
This is body text line 2.
```

Note: If STIG is enabled on the system, you cannot change the default STIG banner.

```
accessclus> system banner set
ACCESS Banner ERROR V-493-10-0 The banner cannot be set as STIG is enable
on the cluster.
```

Managing the password policy using the UI

You can customize the password policies by setting rules for the passwords that are used by the Access Appliance local users. You can set rules for password

complexity, password age, and password lockout. Password complexity specifies the number and type of characters a password must include. Password age defines the duration for which the password is valid. Password lockout specifies the number of failed attempts because of incorrect usage of passwords after which a user is prevented from logging in to the account.

The default password policy for a local user is as follows:

Password complexity:

- Minimum characters: 8
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 1

To change the password policy:

1. Log in to the web interface of a configured Access Appliance cluster by opening a supported browser and typing:

   `http://`*`console-ip`*`:14161`

   where *console-ip* is the management console IP address where the web interface is hosted.
2. In the left navigation pane, click **Settings** and then click **User management**.
3. Click **Manage password policy**.
4. On the Manage password policy page, click **Edit**.
5. If you want your password policy to comply with STIG, select **Reset to STIG default values** to fill in the default values for all the parameters.

   Selecting this option enforces a higher security password policy.
6. Edit the parameters as required. To ignore a rule, leave the corresponding parameter blank. After making the changes click **Save**.

Table 6-1

Parameter	Description
Minimum characters	Minimum number of characters to include in a password
Minimum uppercase characters	Minimum number of uppercase characters to include in a password

Table 6-1 *(continued)*

Parameter	Description
Maximum repetitive characters of the same class	Maximum number of consecutive uppercase, lowercase, numeric, and special characters
Minimum numbers	Minimum number of numeric characters
Minimum special characters	Minimum number of special characters in a password
Minimum character classes	Minimum character classes to include in a password. Character classes include uppercase, lowercase, numeric, and special characters.
Minimum lowercase characters	Minimum number of lowercase characters
Maximum repetitive characters	Maximum number of characters that can be repeated in a password.
Character difference with old password	Number of characters the new password must differ by from the previous password
Days after which password can be changed	Number of days after which a password can be changed
Days after which password must be changed	Number of days after which a password must be changed
Days before warning message	Number of days before the password expires to display a warning
Minimum different passwords before allowing reuse	Number of unique passwords before a previous password can be reused
Number of incorrect login attempts before lockout	Number of failed login attempts after which the account gets locked From version 8.2, when you enable STIG or set the password policy, the SSH session is terminated each time you enter an incorrect password. You must open a new SSH session to log on. Previously, the SSH session was terminated only after the total number of failed attempts was reached.
Time before locked account is reenabled	Duration in seconds the account remains locked

Table 6-1 *(continued)*

Parameter	Description
Time between login failures before account lockout	Number of seconds between consecutive failed login attempts

To change the maintenance user password

1. Login to GUI with maintenance user credentials.
2. Select the **Change password** option.
3. Enter the new password. Click **Save**.

To modify the password policy irrespective of the STIG setting

1. Login to GUI with appliance administrator credentials.
2. Navigate to **Settings > User Management**. Select **Manage password policy**.
3. Edit the settings and click **Save**.

   If you do not want a password expiry date, edit the **Days after which password must be changed** field and leave it empty. Click **Save** to save your changes.

Managing the password policy from the command-line interface

You can customize the password policies by setting rules for the passwords that are used by the Access Appliance local users. You can set rules for password complexity, password age, and password lockout. Password complexity specifies the number and type of characters a password must include. Password age defines the duration for which the password is valid. Password lockout specifies the number of failed attempts because of incorrect usage of passwords after which a user is prevented from logging in to the account.

Commands to view and set the password policy

To view the password policy, use the following command:

```
system password-policy get
```

To set the password policy, use the following command:

```
system password-policy set minlen ucredit maxclassrepeat dcredit
ocredit minclass lcredit maxrepeatdifok pass_min_days pass_max_days
pass_warn_age remember deny unlock_time fail_interval
```

where

Table 6-2

Parameter	Description
minlen	Minimum characters. Range is 6 - 100.
ucredit	Minimum upper case characters. Range is 1 - 100 .
maxclassrepeat	Maximum repetitive characters of same class. Range is 1 - 100.
dcredit	Minimum numbers. Range is 1 - 100.
ocredit	Minimum special characters. Range is 1 - 100.
minclass	Minimum character classes. Range is 1 - 4.
lcredit	Minimum lower case characters. Range is 1 - 100.
maxrepeat	Maximum repetitive characters. Range is 1 - 100.
difok	Character difference with old password. Range is 1 - 100.
pass_min_days	Days after which password can be changed. Range is 1 - 100.
pass_max_days	Days after which password must be changed. Range is 1 - 100.
pass_warn_age	Days before warning message Range is 1 - 100.
remember	Minimum different password before allowing reuse. Range is 1 - 100.
deny	Number of incorrect login attempts before lockout. Range is 1 - 100. From version 8.2, when you enable STIG or set the password policy, the SSH session is terminated each time you enter an incorrect password. You must open a new SSH session to log on. Previously, the SSH session was terminated only after the total number of failed attempts was reached.
unlock_time	Time before locked account is reenabled(seconds). Range is 1 - 604800.
fail_interval	Time before login failures before account locked out (seconds). Range is 1 - 3600.

To display the current password policy:

1. Log on to the Access command-line interface by opening an SSH session to the management console IP as an administrator.
2. In the Access command-line interface, run the following command:

```
system password-policy get
```

```
access-clus> system password-policy get
Password policy setup on the system...
Password complexity:
====================
Minimum characters:                                              8
Minimum upper case characters:                                   1
Maximum repetitive characters of the same class:                 -
Minimum numbers:                                                 1
Minimum special characters:                                      1
Minimum character classes:                                       -
Minimum lower case characters:                                   1
Maximum repetitive characters:                                   -
Character difference with old password:                          -
Password age:
=============
Days after which password can be changed:                        -
Days after which password must be changed:                       -
Days before warning message:                                     -
Minimum different password before allowing reuse:                -
Password lockout:
=================
Number of incorrect login attempts before lockout:               -
Time before locked account is reenabled(seconds):                -
Time before login failures before account locked out(seconds):   -
```

Note: Initially, the default set rules are displayed.

To set the password policy:

1 Log on to the Access command-line interface by opening an SSH session to the management console IP as an administrator.

2 In the Access command-line interface, run the following command:

```
system password-policy set
```

For example:

```
access-clus> system password-policy set minlen=8 ucredit=1
maxclassrepeat=4 dcredit=1 ocredit=1 minclass=4 lcredit=1
maxrepeat=2 difok=8 pass_min_days=1 pass_max_days=60
pass_warn_age=7 remember=7 deny=3 unlock_time=300
fail_interval=900
Access Appliance password-policy SUCCESS V-493-10-0 Password
policy updated successfully.
```

The newly set policy can be displayed using the `system password-policy get` command:

```
access-clus> system password-policy get
Password policy setup on the system...
Password complexity:
====================
Minimum characters:                                          8
Minimum upper case characters:                               1
Maximum repetitive characters of the same class:             4
Minimum numbers:                                             1
Minimum special characters:                                  1
Minimum character classes:                                   4
Minimum lower case characters:                               1
Maximum repetitive characters:                               2
Character difference with old password:                      8
Password age:
============
Days after which password can be changed:                    1
Days after which password must be changed:                   60
Days before warning message:                                 7
Minimum different password before allowing reuse:            7
Password lockout:
=================
Number of incorrect login attempts before lockout:           3
Time before locked account is reenabled(seconds):            300
Time before login failures before account locked out(seconds):  900
```

Note: If STIG is enabled on the system, you cannot change the custom password-policy rules.

```
accessclus> system password-rules set maxrepeat=3
maxclassrepeat=vxdefault dcredit=vxdefault minlen=15
ucredit=vxdefault ocredit=vxdefault lcredit=vxdefault
difok=vxdefault minclass=5 pass_min_days=vxdefault
pass_max_days=vxdefault pass_warn_age=vxdefault deny=3
unlock_time=vxdefault fail_interval=vxdefault remember=vxdefault
ACCESS PasswordRules ERROR V-493-10-0 The password rules cannot
be set as the cluster is STIG enabled.
```

Note: Setting the parameter to **vxdefault** is equivalent to setting the value to **no** or **None**.

Support for immutability in Access Appliance

Immutability support for backup images requires locking down the appliance and not permitting any operations that can lead to data destruction. When the appliance is placed in lockdown mode, administrators are prevented from making any changes to the operating system and the internal components.

Important features:

- Immutable data support with retention locking
- Retention lock deletion for backup images
- Access to Remote Management Platform (HP ILO)
- Transition between different modes
- Retention lock extension

About lockdown modes

Lockdown mode protects your cluster data from internal and external threats by securing all the external endpoints from unauthorized access. Access to all the services is protected and authenticated.

Access 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 the 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, you must contact Veritas Technical Support to obtain a access key and temporarily unlock the appliance. This functionality prevents unauthorized changes even if a malicious actor gained access to stolen credentials.
- It gives the appliance users options for managing WORM (Write Once Read Many) data. Your data is protected from being encrypted, modified, and deleted using WORM properties.

Different lockdown modes provide different level of granularity for WORM and retention. The Access Appliance support three lockdown modes.

- **Normal mode**:
  This is the default mode of the cluster if the lockdown mode is not specified during installation. In this mode, WORM and retention capabilities are disabled. User cannot create WORM STUs and WORM-enabled files/objects in this mode.
- **Enterprise mode**:
  In this mode, WORM and data retention features are enabled. User can choose to create WORM enabled STUs, files and objects. Also, in this mode user has the option to remove the retention locks and expire image data. The user can extend the retention period but cannot reduce the retention period.
  The retention time period can be extended from the WORM enabled STUs and files/objects within them only if the user has the Appliance administrator role.
- **Compliance mode**:
  In this mode, WORM and data retention features are enabled. The user can extend the retention period. The user does not have the option to remove retention locks and expire image data from underlying files/objects of WORM STUs and backup images before the predefined time. Once the appliance lockdown mode is set to compliance, the user does not have the option to delete data until it is expired.

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

Selecting or changing the lockdown mode

The user can select the lockdown mode during initial configuration. After cluster configuration, user has the option to see/change the lockdown mode using the GUI

as well as CLISH. The user can switch between the following modes without any restriction:

- From Normal to Enterprise mode
- From Normal to Compliance mode
- From Enterprise to Compliance mode

You can change the mode from Enterprise to Normal, from Compliance to Normal or from Compliance to Enterprise only if:

- Locked data is not present in deduplication storage or deduplication is not configured in WORM mode.
- WORM enabled file system for any other use cases, such as NFS are not present.
- WORM policies are not activated in the GUI.
- All the file systems are not in offline state.

The user can set minimum and maximum retention time for backup images in Enterprise and Compliance mode only. The retention period range is between 1 hour and 60 years. The retention period can be in second(s) or hour(s) if you use CLISH. The retention period can be in hour(s), day(s), month(s), or year(s) if you use the GUI. Creation of images with retention time less than the minimum retention time or greater than the maximum retention time is not allowed. This minimum and maximum retention time should be set by the appliance administrator as per the retention requirement of their use case.

If Enterprise or Compliance mode has been configured, retention values can be set on files and objects within the range of the minimum retention period and maximum retention period of the WORM-enabled shares or S3 buckets in which they are present.

- Once the lockdown mode is set, only Appliance administrators can change the lockdown mode.
- The lockdown modes are maintained during upgrade.
- Only the Appliance administrator can remove the retention locks if the lockdown mode is enterprise.
- The user cannot change the mode if any existing operation is in progress.

To change the lockdown mode using the GUI

1. Go to **Settings** > **Security management** > **Immutability** and click **Lockdown** mode.
2. On the Lockdown mode page, click **Edit**.
3. Select the mode that you want to enable and click **Save**.

You can also modify the lockdown mode using the `cluster lockdown-mode` commands from CLISH.

```
cluster> lockdown-mode set <mode> [minret] [maxret]
```

Where

mode	Specifies the lockdown mode [normal | compliance | enterprise]
minret	Specifies the minimum retention value range
maxret	Specifies the maximum retention value range

You can also list the lockdown configuration of a cluster using the `cluster lockdown-mode get` command.

Restrictions in different modes

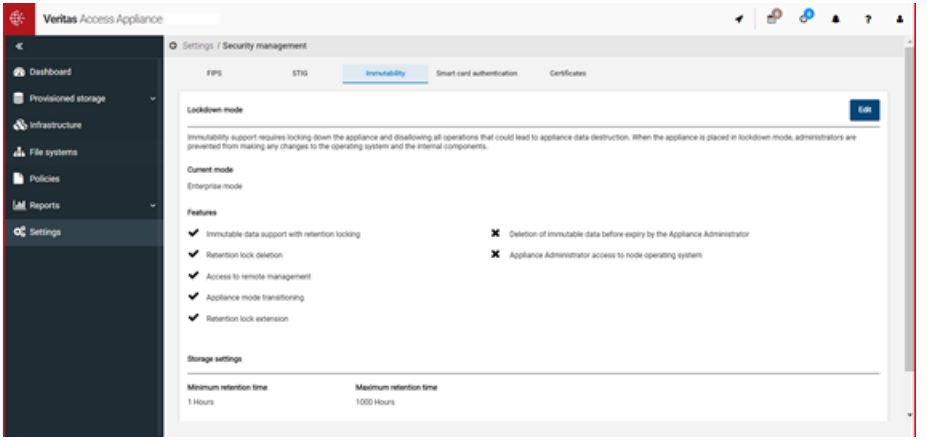
- If lockdown mode is set to compliance or enterprise for any node, it is not available for factory reset.
- During add and replace node operations, the new node is automatically placed in the existing lockdown mode of the cluster. The lockdown mode of the replaced node is set to normal and the node is available for factory reset.
- Cluster maintenance shell is enabled with two-factor authentication (2FA).
- The lockdown mode settings are done at a cluster level and are applicable for all the services, such as NFS that are configured on that cluster.

Configuring immutability using GUI

You can configure immutability using the Access Appliance GUI.

To configure immutability using GUI

1 Go to **Settings** > **Security management** > **Immutability**. Click **Edit**.

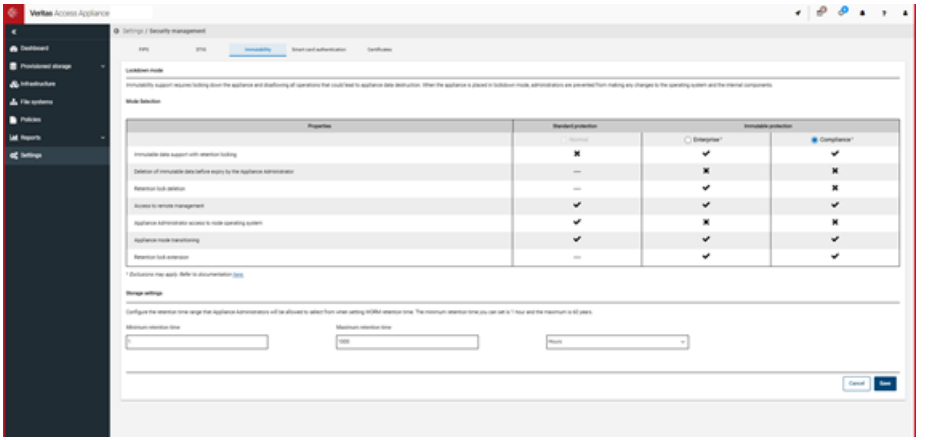


2 Choose any of the lockdown modes under **Mode Selection**. You can choose from Normal, Enterprise and Compliance. The supported features for each mode are listed.

3 If you choose Enterprise or Compliance mode, you also have to configure the retention time range from which the appliance administrators will be allowed to select when creating backup images.

These values will also be used as default values while provisioning storage for different use-cases (such as NFS) from GUI.

Specify the maximum and minimum retention time. These modes also lock down the system and disable immutable data destruction operations. Click **Save**.



Note: Ensure that the image retention period in backup policies is within the lockdown mode retention time to avoid any error during backup.

About system certificates on Access Appliance

Access Appliance supports one certificate for all services (GUI and Object Access). The certificate can be internal or external. The Appliance CA creates the internal certificate. Any CA can create the external certificate using a CSR generated using the Access Appliance GUI. The admin user can get the CA certificate, information about the certificate mode, and expiration using the `system certificate show` command. The CA certificate can also be downloaded using the GUI by navigating to **Settings > Security Management > Certificates**.

The admin user can change the certificate mode using the `system certificate mode set` command. Or you can navigate to **Settings > Security Management > Certificates** in the GUI.

After changing the certificate mode, the admin user should restart all the services to start using the new certificate. The admin user can restart the Object Access service using the following commands:

```
ObjectAccess> server stop
ObjectAccess> server start
```

The admin user can restart the GUI service by navigating to **System > guidisable** and **System > guienable**. You can use the `system certificate mode show` command to get the system certificate mode.

Internal Certificates

If the system certificate mode is set to internal, the certificate that is signed by the Access Appliance CA is used for all the Object Access and GUI services. The admin user has to renew the certificate if the Object Access endpoints get changed using `system certificate renew` command. After the certificate is renewed, the admin user must restart Object Access and GUI service.

Note: The `system certificate renew` command can be used only when the certificate mode is set to internal.

Note: You must update the clients trust-store with CA certificate to secure connection.

About external certificates on Access Appliance

Starting from the Access Appliance 8.1 release, you can generate and use external certificates instead of internal certificates. External Certificate Authority (ECA) certificates are the digital credentials that attest to the certificate owner's identity and affiliation. Once you deploy the external certificates, all the Access Appliance components use them. One certificate is deployed for all the components. These certificates are used by Access Appliance web server and S3 server for a secure client-server communication.

The external certificates also deploy a certificate bundle and (optionally) certificate revocation list. To generate an external certificate, you have to create a certificate request with proper ‘Subject Distinguished Name’ and ‘Subject Alternative Names.’ You can generate a certificate request using the GUI. The necessary FQDNs are auto-populated to generate the correct request. You can add additional information as needed. Based on the certificate request, you can create an external certificate. When deploying external certificate for the first time, you have to provide a CA

certificate bundle. This is used to validate the incoming and deployed external certificate. You can also optionally provide a certification revocation list.

Some important terminologies:

- A certificate authority, also known as a certification authority, is a trusted organization that verifies websites (and other entities) so that you know who you are communicating with online. Their objective is to make the internet a more secure place for both organizations and users. Becoming a Certificate Authority (CA) means that you (or your customers) oversee the issuing process of cryptographic pairs of private keys and public certificates.
- Certificate bundle (CA bundle) is a file that contains root and intermediate certificates. The end-entity certificate along with a CA bundle constitutes the certificate chain.
- Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted. CRL is optional. It may be provided as a file or embedded in certificate as a URL.
- Subject Alternative Name: This field lets you specify additional host names (such as sites, IP addresses, common names, and S3 endpoints) to be protected by a single SSL certificate.

Considerations while deploying ECA:

- All certificates for communication should be obtained from a common trusted CA.
- After ECA is deployed on the cluster, you can renew or update the ECA.
- It is recommended to pause backup/restore operations before starting ECA deployment/renewal.
- The CA bundle and CRL file independent of other security artifacts.
- When you deploy security artifacts, they are validated and if inconsistencies are found, you are notified, and deployment does not proceed. If you provide an external certificate and CA certificate bundle, the EC certificate is validated against the user provided CA certificate bundle. If only one of the items is provided, it is validated against deployed artifacts.
- You receive continuous alerts and emails for 60 days before external certificates are about to expire. You must get new CA certificates and deploy it again for seamless working of the Access Appliance. If you fail to do so, the web server and S3 server stop working.

Download the Access Appliance root certificate, and add it to your web browser's list of trusted certificate authorities. This prevents your web browser from displaying security warning messages when you access the Access Appliance UI. If the

appliance has been upgraded from any version before 8.1, the internal certificates are updated. You can download the certificate from the GUI by navigating to **Settings > Security management > Certificates > Download root certificate** and upload it in the client trust store for a secure client-server communication.

Deploying ECA using the GUI

You can perform all external certificates-related operations from the **Settings** > **Security management** > **Certificates** tab.

- Switch to external certificate
  - Once the external certificates are deployed, user can switch in between internal and external certificates.
  - After the external certificates are deployed, the **Switch to appliance certificates** option is enabled. The web server is restarted after certificates are switched.
  - Internal certificates or appliance certificates are the Access Appliance CA certificates which are deployed during the initial configuration.
- Upload certificate
  - An ECA that is certified to work with CA bundle and an optional certificate revocation list (CRL) is required for the Access Appliance cluster components to use an external certificate.
  - All the artifacts must be deployed in tandem for the first time. This includes external certificate, CA bundle, and CRL.
  - CRL is optional. It may be provided as a file or embedded in certificate as a URL.
  - If using your own certificate, include the certificate and provide a key. Keep the private key unencrypted.
  - Once deployed all the Access Appliance components - web server and S3 services use the external certificates.
  - The web server and S3 server are restarted after deployment of certificate artifacts is successful.
- View certificate request
  - You can view the generated certificate request and verify the subject distinguished names and subject alternative names.
  - You can also copy the generated certificate request and get the CA certificate from it.

- Generate certificate request
  - You must provide a proper subject distinguished name and subject to generate correct external certificate that can be used in Access Appliance cluster.
  - You can use the GUI wizard to generate a proper request for the cluster. The wizard auto populates necessary IP/FQDN to generate correct request.

To deploy ECA using the GUI

1. Go to the **Settings** > **Security Management** > **Certificates** tab.
2. Click **Generate certificate request** and fill out the form. The SAN field is filled with default SAN entries that are mandatory for the configuration. For standard default configuration, it has the FQDN entries for all the storage servers, console IP and API gateway FQDN.
3. Click **Generate** to generate a certificate request.
4. Click **Copy** to copy the certificate request. This has to be given to a CA signing authority who uses this to generate a certificate. CA signing authority provides a certificate along with the root certificate and intermediate certificate used to generate the certificate. Authority may also provide a CRL file .
5. You also have an option to upload a private key. If you want to use your own certificate, include the certificate and provide a key. Ensure that the private key is unencrypted.
6. Go to **Certificates** > **Upload certificate** to upload the certificate artifacts. For a fresh deployment, both the certificate and CA certificate bundle are mandatory. CRL is optional. For renewal, any one of the three are required.
7. After the certificate is uploaded, **Save** gets enabled. Click **Save**. The deployment is initiated.

   After deployment is successfully completed for all components, the GUI restarts with the uploaded external certificate.

You can verify the browser certificate from the GUI to verify that it is the same one that was used during deployment.

Log locations

You can find the logs at the following locations:

- The configuration file can be found at `/shared/cluster_certs/external/config.json`. It contains information such as CSR, and whether ECA is deployed.
- The deployed artifacts can be found at `/shared/cluster_certs/external/`.

- All the logs pertaining to ECA deployment are present in the `/log/VRTSnas/log` directory.
- `/opt/VRTSnas/log/va_external_certificates.log` contains the logs of the driver script which is responsible for performing pre-checks and then calling subsequent scripts to deploy ECA on various components.

About single sign-on (SSO) configuration

You can configure single sign-on (SSO) with any identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Cohesity product. Access Appliance supports ADFS, Okta, Azure, and Ping Federate IDPs in this release.

Note the following requirements and limitations:

- To use SSO, you must have a SAML 2.0 compliant identity provider configured in your environment.
- Configuration of the IDP requires the Access Appliance GUI.
- Global logout is not supported.
- SSO is supported only for AD/LDAP users.

Configuring SSO on Access Appliance

Configuring SSO on Access Appliance involves the following steps:

Table 6-3

Task	Description
Configuring SSO on an Access Appliance cluster	See To configure SSO on an Access Appliance cluster
Adding users/group	See “Adding and removing user roles using GUI” on page 285.
Configuring an identity provider	See To configure an identity provider
Logging into Access Appliance with SSO	See Login with SSO

Configuring SSO on an Access Appliance cluster

To configure SSO on an Access Appliance cluster

1. Go to **Settings > Security management > Single sign-on (SSO)**. Click **Add**.
2. Give the IDP name and upload the IDP metadata xml and optionally provide the custom user field and group field values. The user field and group field values should be same as configured on the IDP. Click **Save**.

   The UI displays a message that confirms that the add identity provider task is triggered. You can click **View Details** to see the progress of the task. Alternatively, you can also click the **Recent Activity** icon from the top right of the UI to see the status of the most recent operations.
3. Once the configuration is complete, the SSO identify provider details are displayed on the screen. Click **Download service provider xml** to download the details and upload it on IDP server, if required.

Configuring an identity provider

To configure an identity provider

- Login with SSO works only if the configuration on the IDP side is done. Each IDP has different steps for configuration.

  Note: The IDP should always sign the assertation to ensure that the configuration is trustworthy.

  Refer to the following links for the configuration steps for each identity provider.

  - ADFS: Enrolling Access Appliance primary server as a service provider to ADFS
  - Azure: Enrolling Access Appliance primary server as a service provider to Azure
  - Okta: Enrolling Access Appliance primary server as a service provider to Okta
  - Pingfederate: Enrolling Access Appliance primary server as a service provider to Pingfederate

Logging into Access Appliance with SSO

Login with SSO

1. Navigate to GUI login page. Click **Sign-in with single sign-on (SSO)**.
2. Enter SSO credentials and click **Sign in**.

Adding and removing user roles using GUI

You can use the Access Appliance GUI to add local, AD and LDAP users.

To add a new user

1. Navigate to **Settings** > **User management** and click **Add** to add a new user.
2. The **Add user** form appears.
   - To add a local user, select the user type as **Local**.
   - To add an AD/LDAP user, select the user type as **Directory** and add a valid user name or group name.
   - For AD, enter **domain\\username**.
   - For LDAP, enter **username**.

   Click **Add**.
3. The list of users gets updated after the operation is complete.

To remove a user

1. You can remove a user by clicking the menu button next to the user and selecting **Remove**.
2. A confirmation window appears. Click **Ok** to remove the user. The list of users gets updated after the operation is complete.

Limitations and log locations

There are some limitations when you configure SSO on an Access Appliance cluster.

- Identity provider cannot be edited. It can be removed and added again.
- Single logout is not implemented. If SAML users log out of the application, and try to login with SSO again, the user is not asked for their login credentials unless the SSO session has expired. This applies to any other application using the same IDP.
- If after identity provider configuration, External certificate authority (ECA) is configured, then login with SSO does not work until the identity provider is updated with the latest service provider metadata xml from the Access Appliance. This can be done by downloading the service provider metadata xml from **Settings > Security > Single-Sign on > Download service provider metadata**. This metadata needs to be updated on the IDP side.
- AD/IDP server date, time, and time zone should be the same as the Access Appliance cluster. Else, the SSO login fails.

The logs can be found by logging into the Access Appliance CLISH, elevating to root and accessing the logs at:

- `/log/VRTSnas/isagui_webserver.log`
- `/log/VRTSnas/ isagui_sso_config.log`

Configuring user authentication using digital certificates or smart cards

You can configure NetBackup to authenticate users with a smart card or a digital certificate. After configuration, the users can use the **Sign in with certificate or smart card** option to sign in to NetBackup UI using smart cards or digital certificates.

Before you configure user authentication using smart cards or digital certificates, note the following:

- Digital certificate or smart card authentication can be configured for LDAP, AD, and local users.
- To authenticate LDAP users using digital certificate or smart card, ensure that LDAP is configured. Go to **Settings > Directory Services management** and click **Configure** to configure LDAP, if not already done so. For details about how to configure LDAP:
  See "About configuring LDAP settings" on page 288.
  See "Configuring LDAP server settings" on page 289.
- To authenticate AD users using digital or smart, ensure that AD is configured. Go to **Settings > Directory Services management** and click **Configure** to configure AD, if not already done so. For details about how to configure AD:
  See "Configuring AD server settings" on page 292.
- To authenticate local users using digital or smart card, ensure that you create a local user. Go to **Settings > User management > Add**.
- Smart card authentication requires a list of trusted root or intermediate CA certificates. You must add the CA certificates that are associated with the user digital certificates or the user smart cards.

To configure NetBackup to authenticate users with a certificate or smart card:

1. Log in to NetBackup UI.
2. In the left navigation pane, click **Settings > Security management**, and then click **Smart card authentication**.
3. Use the slider to turn on smart card authentication.

4. In the **Configure smart card authentication** dialog box, specify the following options:
   - In the user authentication domain list:
     - For local user select none.
     - For an AD user, select the configured AD server.
     - For an LDAP user, select the configured LDAP server.
   - Click **Common name** to select the common mapping attribute.
   - Optionally, enter the Online Certificate Status Protocol (OCSP) URI. OSCP is used for checking the validity of the certificate.
     If you do not provide the OCSP URI, the URI in the user certificate is used.
5. Click **Save**.
6. To the right of **CA certificates** click **Add**.
7. Click **Browse** to select the CA certificate or drag and drop the CA certificate and click **Add**.

   Certificates must be in PEM format, with certificate file type as `.pem`. Only one certificate can be added at a time. The web server is restarted after adding the certificate.

   The selected CA certificate is displayed under **CA certificates**.
8. Upload the client certificate to the browser's certificate store. See the browser documentation for importing client certificates.

The users can now use the **Sign in with certificate or smart card** option to sign in to the NetBackup UI. LDAP users with Appliance administrator role have access to all the settings in the UI. LDAP users that do not have this role can only create S3 keys. AD users with Appliance administrator role have access to all the settings in the UI. AD users that do not have this role can only create S3 keys. Local users with Appliance administrator role have access to all the settings in the UI. Local users that do not have this role have access only to change password screen.

Adding CA certificates for smart card authentication

Smart card authentication requires a list of trusted root or intermediate CA certificates. Add the CA certificates that are associated with the user digital certificates or the user smart cards.

To add a CA certificate:

1. Log in to NetBackup UI.
2. In the left navigation pane, click **Settings > Security management**, and then click **Smart card authentication**.
3. To the right of **CA certificates** click **Add**.
4. Click **Browse** to select the certificate or drag and drop the CA certificate and click **Add**.

   The web server is restarted after adding the certificate.

   The selected certificate is displayed under **CA certificates**.

Deleting CA certificates

You can delete a CA certificate if it is no longer used for smart card authentication. If a user attempts to use the associated digital certificate or smart card certificate, they are not able to sign in to NetBackup.

To delete a CA certificate:

1. Log in to NetBackup UI.
2. In the left navigation pane, click **Settings > Security management**, and then click **Smart card authentication**.
3. Select the CA certificate that you want to delete and click **Delete**.

   The certificate is deleted and no longer displayed under **CA certificates**. The web server is restarted after the certificate is deleted.

About configuring LDAP settings

The Lightweight Directory Access Protocol (LDAP) is the protocol used to communicate with LDAP servers. The LDAP servers are the entities that perform the service. In Access Appliance, the most common use of LDAP is for user authentication.

For sites that use an LDAP server for access or authentication, Access Appliance provides a simple LDAP client configuration interface.

Before you configure Access Appliance LDAP settings, obtain the following LDAP configuration information from your system administrator:

- IP address or host name of the LDAP server. You also need the port number of the LDAP server.
- Base (or root) distinguished name (DN), for example:

```
cn=employees,c=us
```

LDAP database searches start here.

- Bind distinguished name (DN) and password, for example:

  ```
  ou=engineering,c=us
  ```

  This allows read access to portions of the LDAP database to search for information.

- Base DN for users, for example:

  ```
  ou=users,dc=com
  ```

  This allows access to the LDAP directory to search for and authenticate users.

- Base DN for groups, for example:

  ```
  ou=groups,dc=com
  ```

  This allows access to the LDAP database, to search for groups.

- Base DN for Netgroups, for example:

  ```
  ou=netgroups,dc=com
  ```

  This allows access to the LDAP database, to search for Netgroups.

- Root bind DN and password. This allows write access to the LDAP database, to modify information, such as changing a user's password.
- Secure Sockets Layer (SSL). Configures a cluster to use the Secure Sockets Layer (SSL) protocol to communicate with the LDAP server.

Configuring LDAP server settings

You can set the LDAP base Distinguished Name (base DN). LDAP records are structured in a hierarchical tree. You access records through a particular path, in this case, a Distinguished Name, or DN. The base DN indicates where in the LDAP directory hierarchy you want to start your search.

Note: For Access Appliance to access an LDAP directory service, you must specify the LDAP server DNS name or IP address.

To set the base DN for the LDAP server

- To set the base DN for the LDAP server, enter the following:

  ```
  Network> ldap set basedn value
  ```

  where *value* is the LDAP base DN in the following format:

  ```
  dc=yourorg,dc=com
  ```

To set the LDAP server hostname or IP address

- To set the LDAP server hostname or IP address, enter the following:

  ```
  Network> ldap set server value
  ```

  where *value* is the LDAP server hostname or IP address.

To set the LDAP server port number

- To set the LDAP server port number, enter the following:

  ```
  Network> ldap set port value
  ```

  where *value* is the LDAP server port number.

To set Access Appliance to use LDAP over SSL

- To set Access Appliance to use LDAP over SSL, enter the following:

  ```
  Network> ldap set ssl {on|off}
  ```

To set the bind DN for the LDAP server

- To set the bind DN for the LDAP server, enter the following:

  ```
  Network> ldap set binddn value
  ```

  where *value* is the LDAP bind DN in the following format:

  ```
  cn=binduser,dc=yourorg,dc=com
  ```

  The *value* setting is mandatory.

  You are prompted to supply a password. You must use the password used to connect to the LDAP service on the specified LDAP server.

To set the root bind DN for the LDAP server

- To set the root bind DN for the LDAP server, enter the following:

  ```
  Network> ldap set rootbinddn value
  ```

  where *value* is the LDAP root bind DN in the following format:

  ```
  cn=admin,dc=yourorg,dc=com
  ```

  You are prompted to supply a password. You must use the password used to connect to the LDAP service on the specified LDAP server.

To set the LDAP users, groups, or netgroups base DN

- To set the LDAP users, groups, or netgroups base DN, enter the following:

  ```
  Network> ldap set users-basedn value
  ```

  ```
  Network> ldap set groups-basedn value
  ```

  ```
  Network> ldap set netgroups-basedn value
  ```

users-basedn *value*	Specifies the value for the users-basedn. For example: `ou=users,dc=example,dc=com (default)`
groups-basedn *value*	Specifies the value for the groups-basedn. For example: `ou=groups,dc=example,dc=com (default)`
netgroups-basedn *value*	Specifies the value for the netgroups-basedn. For example: `ou=netgroups,dc=example,dc=com (default)`

To display the LDAP configured settings

- To display the LDAP configured settings, enter the following:

  ```
  Network> ldap get {server|port|basedn|binddn|ssl|rootbinddn|
  users-basedn|groups-basedn|netgroups-basedn}
  ```

To clear the LDAP settings

- To clear the previously configured LDAP settings, enter the following:

  ```
  Network> ldap clear {server|port|basedn|binddn|ssl|rootbinddn|
  users-basedn|groups-basedn|netgroups-basedn}
  ```

To clear all the LDAP settings

- To clear the LDAP client configuration settings for all parameters, enter the following:

```
Network> ldap clearall
```

Configuring AD server settings

The `network ad` commands are used to configure the Active Directory (AD) client for authentication. These commands configure the Access Appliance to use AD users and groups when logging into the Access Appliance.

If the AD client's domain controller is set to refuse NTLM authentication, run the following command to disable NTLM prior to configuring the Active Directory client:

```
CLFS> set ntlm_auth no
```

To set the AD client configuration

- You can set the AD client's domain, domain controller, workgroup and domain user. To set the AD client configuration details, enter the following:

```
Network> ad set domain domaincontroller workgroup
domainuser idmapupperbound
```

domain	Active Directory domain name or Windows NT domain name
domaincontroller	Primary[,backup] domain-controller names
workgroup	Windows WORKGROUP name or NetBIOS domain name
domainuser	domain user name which is used for authentication in the domain join operation
idmapupperbound	idmap upper bound for AD users

Access Appliance displays the cluster time as well as the time on the Active Directory Domain Controller.

If NTP has been configured correctly, there will be no time skew. Otherwise, you will need to reconfigure NTP correctly.

You will be prompted to enter the password of `domainuser`.

To enable the AD client

- To enable the AD client to use Active Directory for authentication, enter the following:

```
Network> ad enable
```

To display the AD client configuration

- To display the AD client configuration, enter the following:

```
Network> ad show
```

To disable the AD client

- To disable the AD client so that Active Directory is not used for authentication, enter the following:

```
Network> ad disable
```

To clear the AD client configuration

- To clear the AD client configuration, enter the following:

```
Network> ad unset
```

About multifactor authentication

Multifactor authentication is a robust security measure widely used for adding an additional layer of security to the authentication process by requiring users to provide a unique, time-limited code along with their regular login credentials. It is a multiple-step account login process that requires you to enter a 6-digit one-time password along with your password.

It is strongly recommended that you configure multifactor authentication to protect the security of your account.

See "Configuring multifactor authentication for your user account" on page 294.

If multifactor authentication is enforced in the Access Appliance cluster, all users must configure multifactor authentication for their user accounts for successful sign-in.

See "Configuring multifactor authentication for your user account when it is enforced in the cluster" on page 296.

Considerations when configuring multifactor authentication

Some considerations that you need to remember before you configure multifactor authentication:

- The Appliance administrator can see the status of all the users on the **Settings > User management** page.
- If AD/LDAP server configuration is removed from the cluster without removing the AD/LDAP user's multifactor authentication configuration, the Appliance administrator may see stale entries for AD/LDAP users.
- Multifactor authentication configuration for AD/LDAP users with no role is only possible after multifactor authentication enforcement.
- A local administrator is a non AD/LDAP user.
- Do not configure multifactor authentication if `add node` or `delete node` operations are in progress.

Perform the following steps to login to the Swagger REST APIs if multifactor authentication is configured for a particular user:

- Provide username (for which multifactor authentication is configured) and password and generate token. A token of the type, *mfa token*, is generated.
- Copy the token and paste it in the username field. Provide the OTP received in the authentication app in the password field, and enter *mfa* in the token type field.
- A bearer token is generated for that user. This token should be provided in the **Authorize** tab with the format as: *Bearer <bearer token>*.

Configuring multifactor authentication for your user account

You must first install and configure authenticator application on your smart device that provides you with the one-time password.

Supported authenticator applications

If the Access Appliance administrator has enforced multifactor authentication in the Access Appliance cluster, you must configure it for your user account for successful sign-in. You must configure multifactor authentication before the start date of enforcement. Else, you will lose access to the appliance and your automation workflow (if using login API) will also be impacted.

Even if multifactor authentication is not enforced, it is recommended that you configure it for enhanced security.

To configure multifactor authentication for your user account

1. Sign in to the Access Appliance UI.
2. On the top right, click the profile icon and click **Manage multifactor authentication**.
3. On the **Manage multifactor authentication** screen, click **Configure**.
4. On the next screen, follow the given steps.

   Install and configure authenticator application on your smart device. It generates one-time password and sends it on your smart device.
5. Scan the QR code with the authenticator application or enter the key manually.

   The manual key should be base32 encoded and can contain between 26 to 208 characters with or without padding.
6. Enter the one-time password that you see in the authenticator application.
7. Click **Configure**.

   At the time of next sign-in, you need to enter the one-time password along with the username and password.

See "Disabling multifactor authentication for your user account" on page 295.

Disabling multifactor authentication for your user account

You can disable MFA for your user account only if multifactor authentication is not enforced. However, it is strongly recommended that you configure multifactor authentication to protect the security of your account.

If multifactor authentication is enforced, and you want to reset it, See "Resetting multifactor authentication for a user" on page 297.

To disable multifactor authentication for your user account

1. Sign in to the Access Appliance UI.
2. If you are an Appliance administrator, click the profile icon on the top right, and select **Manage multifactor authentication**.

   If you are not an Appliance administrator, select **Manage multifactor authentication** in the home screen.
3. If you have already configured multifactor authentication for your user account, you can see the **Disable** button.
4. Click **Disable**.
5. Enter the one-time password and click **Submit**.

Enforcing multifactor authentication for all users

Only the Access Appliance administrator can enforce multifactor authentication for all Access Appliance users.

Before you enforce multifactor authentication:

- Multifactor authentication can be enforced only if at least two local Appliance administrator users have configured it.
- You can set a future start date for enforcement so that the users get sufficient time to configure their multifactor authentication.
- If multifactor authentication is not configured by the start date, the user will not have access to the appliance. If the user's automation workflow uses login API, then that will also be impacted.
- Once multifactor authentication is enforced, it cannot be reversed.
- It is not possible to postpone the start date of enforcement after it is set.
- You can prepone the start date for enforcement using the **Edit enforcement** button on the **Settings > Security management > Multifactor authentication** page.
- The start date for enforcement cannot be more than 90 days from the current date.

To enforce multifactor authentication for all users

1. Sign in to the Access Appliance UI.
2. Go to **Settings > Security management > Multifactor authentication**.
3. Click **Enforce** to enforce multifactor authentication for all Access Appliance users.

   Notify all users that they must configure multifactor authentication for their user accounts to be able to successfully sign in.

   See "Configuring multifactor authentication for your user account" on page 294.

Configuring multifactor authentication for your user account when it is enforced in the cluster

After multifactor authentication is enforced in the cluster, you must configure it for your user account if you have not already configured it.

If you have not configured multifactor authentication for your account after the enforcement, you cannot sign-in to the appliance if the enforcement period has expired and any automation workflow using the login API will be impacted. If the enforcement period has not expired, you can skip the multifactor authentication

configuration in the login screen but it is recommended that you configure multifactor authentication to protect the security of your account.

To configure multifactor authentication after the enforcement

1. Open a web browser and go to the following URL.

   https://*console-IP*:14161/login

   The *console-IP* is the management console IP address where the web interface is hosted.

2. Enter the **Username** and **Password**.
3. Click **Sign in**. The **Configure multifactor authentication** screen is displayed.
4. On the next screen, follow the given steps.

   Install and configure an authenticator application on your smart device. It generates a one-time password and sends it to your smart device.

   Supported authenticator applications

5. Scan the QR code with the authenticator application or enter the key manually.

   The manual key should be base32 encoded and can contain between 26 to 208 characters with or without padding.

6. Enter the one-time password that you see in the authenticator application.
7. Click **Submit**.

   Successful configuration takes you back to the sign-in screen.

   Enter the username, password, and one-time password for successful sign-in.

Resetting multifactor authentication for a user

Only the Access Appliance administrator can reset multifactor authentication for other Access Appliance users.

Before you reset multifactor authentication:

- The logged in administrator cannot reset his own multifactor authentication. It can only be reset by another Appliance administrator.
- If multifactor authentication is not enforced, then it is possible to reset it for any user.
- If multifactor authentication is enforced, then you can reset it for a local (non AD/LDAP) administrator only if at least one other local administrator is present who has multifactor authentication configured.

To reset multifactor authentication for an Access Appliance user

1. Sign in to the Access Appliance UI.
2. Go to **Settings > User management**.
3. Navigate to the user row and click on the vertical ellipsis button from the right side of the UI and then select **Reset multifactor authentication** .
4. In the **Reset multifactor authentication** pop-up, click **Reset**.

Configuring an isolated recovery environment using the command line

See the following topics to configure an isolated recovery environment using the command line:

Table 6-4 IRE configuration using the command line

Task	Description
Configure an isolated recovery environment on a storage server.	See "Configuring an isolated recovery environment on a storage server" on page 298.
Manage an isolated recovery environment on a storage server.	See "Managing an isolated recovery environment on a storage server" on page 302.
Configure the data transmission between a production environment and an IRE storage server.	See "Configuring data transmission between a production environment and an IRE storage server" on page 305.

Configuring an isolated recovery environment on a storage server

You can configure an isolated recovery environment (IRE) on a storage server to create an air gap between your production environment and a copy of the protected data. The air gap restricts network access to the data except during the timeframe when data replication occurs. This feature helps to protect against ransomware and malware.

To configure the IRE, you need a production Access Appliance environment and a target storage server on a supported Cohesity appliance. Check the appliance documentation for compatibility.

The production environment does not require any additional steps for this feature. Use the following procedure to configure an IRE on the target storage server from the MSDP restricted shell. You can login to the MSDP restricted shell by logging

in to the target MSDP server IP (deduplication IP) with credentials of a cluster local user having administrator role.

Note: All the MSDP restricted shell commands should be executed on the IRE/target storage server.

To configure an IRE

1 If A.I.R. is not configured on the production domain, continue to the next step.

If A.I.R. is already configured on the production domain, log in as a local user with administrator role (same user that was used for Access Appliance CLISH login). Run the following command to show the SLP windows for replication from the primary server to the server.

```
setting ire-network-control show-slp-windows
production_primary_server=<production domain>
production_primary_server_username=<production username>
ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
username>
```

Where:

- *<production domain>* is the fully qualified domain name (FQDN) of the primary server in your production environment.
- *<production username>* is the username of the NetBackup primary user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- *<IRE domain>* is the FQDN of the primary server in the IRE. Use the same hostname that you used for the target primary server when you configured the SLPs in the production environment.
- *<IRE username>* is the username of a IRE NetBackup primary user with permission to list SLPs and storage units in the IRE. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.

For example:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=example_user
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=example_user1
```

The following is an example output of the command:

```
EveryDayAtNoon:
SLPs: SLP1
Sunday start: 12:00:00 duration: 00:59:59
Monday start: 12:00:00 duration: 00:59:59
Tuesday start: 12:00:00 duration: 00:59:59
Wednesday start: 12:00:00 duration: 00:59:59
Thursday start: 12:00:00 duration: 00:59:59
Friday start: 12:00:00 duration: 00:59:59
Saturday start: 12:00:00 duration: 00:59:59

WeeklyWindow:
SLPs: SLP2
Sunday start: 10:00:00 duration: 01:59:59
Monday NONE
Tuesday NONE
Wednesday NONE
Thursday NONE
Friday NONE
Saturday start: 10:00:00 duration: 01:59:59
```

This example shows two SLP windows:

- A daily window for one hour starting at noon.
- A weekly window for two hours starting at 10:00 A.M.

2 Based on the requirements for your environment, determine a schedule and take note of it. For an existing A.I.R. environment, the schedule must accommodate the SLP windows that you viewed in the previous step.

You can set a daily schedule that is open at the same time each day, or you can set a different schedule for each day of the week.

In the previous example, you can accommodate both SLP windows with either of the following:

- A daily schedule from 10:00 A.M. to 1:00 P.M.
- A schedule from 12:00 P.M. to 1:00 P.M. on Monday through Friday and a schedule from 10:00 A.M. to 1:00 P.M. on Saturday and Sunday

Note: If the production environment and the IRE are in different time zones, the schedule must begin only once per day in both time zones. For example, if one environment is in the Asia/Kolkata time zone and the other is in the America/New_York time zone, the following schedule in Kolkata is not supported: Tuesday start time 22:00:00 and Wednesday start time 03:00:00. When these start times get converted to the New York time zone, they become Tuesday start time 12:30:00 and Tuesday start time 17:30:00, which is not supported.

3 Run the following command to configure which subnets and IP addresses are allowed to access the storage server:

```
setting ire-network-control allow-subnets subnets=<CIDR subnets
or IP addresses>
```

Where *<CIDR subnets or IP addresses>* is a comma-separated list of the allowed IP addresses and subnets, in CIDR notation.

For example:

```
setting ire-network-control allow-subnets
subnets=10.80.120.208,10.84.48.0/20
```

Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE must be included in the allowed list. If all of these servers are in the same subnet, only the subnet is required to be in the allowed list.

4 Run the following command to set the daily air gap schedule:

```
setting ire-network-control set-schedule start_time=<time>
duration=<duration> [weekday=<0-6>]
```

Where [weekday=<*0-6*>] is an optional parameter to indicate the day if you need to set different schedules for different days. 0 is Sunday, 1 is Monday, etc.

For example:

```
setting ire-network-control set-schedule start_time=10:00:00
duration=03:00:00 weekday=0
```

5 Before you can send data between the production domain and the IRE storage server, you must add MSDP reverse connections and add the replication operation.

See "Configuring data transmission between a production environment and an IRE storage server" on page 305.

Note: When multiple Veritas Data Deduplication instances are configured in an IRE domain cluster, and subnets and schedules are set using the MSDP restricted shell for all the Veritas Data Deduplication instances; if any of the instances is stopped and the cluster is restarted, the outbound connection rules corresponding to that instance is lost after the restart operation. This is by design and the outbound connection rules, if any, are applied back only if the stopped instance(s)are started back.

Managing an isolated recovery environment on a storage server

Once you have configured an isolated recovery environment (IRE) on a storage server, you can manage it from the MSDP restricted shell with a local user with administrator role (same user that was used for Access Appliance CLISH login). Use the following commands.

- To view the SLP windows from the primary server to the server:

  ```
  setting ire-network-control show-slp-windows
  production_primary_server=<production domain>
  production_primary_server_username=<production username>
  ire_primary_server=<IRE domain> ire_primary_server_username=<IRE
  username>
  ```

  Where:

  - *<production domain>* is the fully qualified domain name (FQDN) of the primary server in your production environment.

- *<production username>* is the username of a NetBackup primary user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- *<IRE domain>* is the FQDN of the primary server in the IRE. Use the same hostname that you used for the target primary server when you configured the SLPs in the production environment.
- *<IRE username>* is the username of a IRE NetBackup primary user with permission to list SLPs and storage units in the IRE. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.

For example:

```
production_primary_server=examplePrimary.domain.com
production_primary_server_username=example_user
ire_primary_server=exampleIREPrimary.domain.com
ire_primary_server_username=example_user1
```

Note: The SLP replication window on the production domain must be configured to be open at the same time as the IRE schedule.

- To list the MSDP reverse connections:

```
setting ire-network-control list-reverse-connections
```

- To add an MSDP reverse connection:

```
setting ire-network-control add-reverse-connection
remote_storage_server=<production MSDP server>
[remote_primary_server=<production primary server>]
[local_storage_server=<IRE network interface>]
```

Where:

- *<production MSDP server>* is the FQDN of the MSDP server in your production environment.
- [remote_primary_server=*<production primary server>*] is an optional parameter for the FQDN of the primary server in your production environment. This parameter is required if the IRE domain uses an alternative name to access the production primary server. This scenario usually occurs if the production primary server runs on multiple networks with multiple hostnames.
- [local_storage_server=*<IRE network interface>*] is an optional parameter for the hostname of the network interface to use for image replication on the IRE storage server. This parameter is required if the network interface for replication is different than the IRE storage server name.

- To verify that a reverse connection works:

  ```
  setting ire-network-control validate-reverse-connection
  remote_storage_server=<production MSDP server>
  [remote_primary_server=<production primary server>]
  [local_storage_server=<IRE network interface>]
  ```

- To remove an MSDP reverse connection:

  ```
  setting ire-network-control remove-reverse-connection
  remote_storage_server=<production MSDP server>
  ```

- To view the allowed IP addresses and subnets:

  ```
  setting ire-network-control show-allows
  ```

- To add IP addresses and subnets to the allowed list:

  ```
  setting ire-network-control allow-subnets subnets=<CIDR subnets
  or IP addresses>
  ```

  Where *<CIDR subnets or IP addresses>* is a comma-separated list of the allowed IP addresses and subnets, in CIDR notation.

  For example:

  ```
  setting ire-network-control allow-subnets
  subnets=10.80.120.208,10.84.48.0/20
  ```

  Note: The IRE primary server, the IRE media servers, and the DNS server for the IRE must be included in the allowed list. If all of these servers are in the same subnet, only the subnet is required to be in the allowed list.

- To remove the IP addresses and subnets from the allowed list:

  ```
  setting ire-network-control allow-subnets subnets=,
  ```

- To view the daily air gap schedule:

  ```
  setting ire-network-control show-schedule
  ```

- To change the air gap schedule:

  ```
  setting ire-network-control set-schedule start_time=<time>
  duration=<duration>
  ```

  For example:

  ```
  setting ire-network-control set-schedule start_time=10:00:00
  duration=03:00:00
  ```

- To stop the air gap schedule:

  ```
  setting ire-network-control delete-schedule
  ```

- To view the current network status and check whether the external network is open or closed:

```
setting ire-network-control external-network-status
```

- To manually open the external network:
  ```
  setting ire-network-control external-network-open
  ```
- To manually close the external network and resume the air gap schedule:
  ```
  setting ire-network-control resume-schedule
  ```

Note: The commands may take a few minutes to take effect.

Configuring data transmission between a production environment and an IRE storage server

Once the configuration of an isolated recovery environment (IRE) is completed, the production Access Appliance hosts are no longer able to access the storage server. You need to add MSDP reverse connections to allow data transmission between the production MSDP storage server and the IRE storage server. Then you can add the replication operation.

To configure data transmission between a production environment and an IRE

1. Open an SSH session to the IRE storage server. Run the following command to determine if the external network is open:

   ```
   setting ire-network-control external-network-status
   ```

   If it is not, run the following command:

   ```
   setting ire-network-control external-network-open
   ```

2. Run the following command to add an MSDP reverse connection:

   ```
   setting ire-network-control add-reverse-connection
   remote_storage_server=<production MSDP server>
   [remote_primary_server=<production primary server>]
   [local_storage_server=<IRE network interface>]
   ```

   Where:

   - *<production MSDP server>* is the fully qualified domain name (FQDN) of the MSDP server in your production environment.
   - [remote_primary_server=*<production primary server>*] is an optional parameter for the FQDN of the primary server in your production environment. This parameter is required if the IRE domain uses an alternative name to access the production primary server. This scenario

usually occurs if the production primary server runs on multiple networks with multiple hostnames.

- [local_storage_server=<*IRE network interface*>] is an optional parameter for the hostname of the network interface to use for image replication on the IRE storage server. This parameter is required if the network interface for replication is different than the IRE storage server name.

3 If necessary, repeat the previous step to add additional MSDP reverse connections.

4 If Auto Image Replication (AIR) is not already configured on the production domain, run the following command to copy the IRE schedule to the production domain as a storage lifecycle policy (SLP) window:

```
setting ire-network-control sync-ire-window
production_primary_server=<production primary server>
production_primary_server_username=<production username>
[slp_window_name=<SLP window name>]
```

Where:

- *<production primary server>* is the FQDN of the primary server in your production environment.
- *<production username>* is the username of the NetBackup primary user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- [slp_window_name=<*SLP window name*>] is an optional parameter to give a name for the SLP window. If you do not provide this parameter, the name of the SLP window is `IRE_DEFAULT_WINDOW`.

5 If you do not have them already, create a source SLP on the production primary server and a target import SLP on the IRE primary server.

Note: You cannot add the replication operation from the production NetBackup primary when you create the SLPs as the target storage is air gapped. Continue to the next step to add the replication operation.

---

6 Run the following command to add the IRE storage server as a replication target of the production Access Appliance domain and to add the replication operation to the SLP:

```
setting ire-network-control add-replication-op
production_primary_server=<production primary server>
```

```
production_primary_server_username=<production username>
production_storage_server=<production storage server>
ire_primary_server_username=<IRE username>
source_slp_name=<production SLP name> target_import_slp_name=<IRE
SLP name> target_storage_server=<target storage server>
target_storage_server_username=<target storage server username>
production_storage_unit=<MSDP storage unit> [slp_window_name=<slp
window name>]
```

Where:

- *<production primary server>* is the FQDN of the primary server in your production environment.
- *<production username>* is the username of the NetBackup primary user with permission to list SLPs and SLP windows in the production environment. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- *<production storage server>* is the FQDN of the production storage server in your production environment.
- *<IRE username>* is the username for an administrator on the IRE NetBackup primary server. For Windows users, enter the username in the format ***<domain name>\<username>***. For other users, enter the username only.
- *<source SLP name>* is the SLP name from the production primary server to add the replication operation to.
- *<target SLP name>* is the import SLP name from the IRE primary server.
- *<target storage server>* is the FQDN of the target storage server in your IRE environment.
- *<target storage server username>* is the username of the MSDP storage server used while configuring the target storage server .
- *<MSDP storage unit>* is the name of the MSDP storage unit that is the replication source in the source SLP.
- [slp_window_name=*<slp window name>*] is an optional parameter for the name of the SLP window that is synced with the IRE schedule. This parameter must match the SLP window name from the previous step, if applicable. If you do not provide this parameter, the default name is used.

7 If you opened the external network at the beginning of this procedure, run the following command to close it and resume the air gap schedule:

```
setting ire-network-control resume-schedule
```

Note: The `setting ire-network-control allow-devices` is not supported in Access Appliance.

Forwarding logs to an external server

You can forward system logs to an external log management server. System logs (syslog) contain event and notification messages in a specific format. Forwarding the appliance syslogs to an external log management server provides system administrators a centralized location for viewing logs and for further analysis and troubleshooting. The following log servers are supported:

- HP ArcSight
- Splunk

NetBackup appliances use the Rsyslog client to forward logs. In addition to HP ArcSight and Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance.

To secure the log transmission from the appliance to the log management server, you can use the TLS (Transport Layer Security) option. The NetBackup currently supports only TLS Anonymous Authentication for log forwarding.

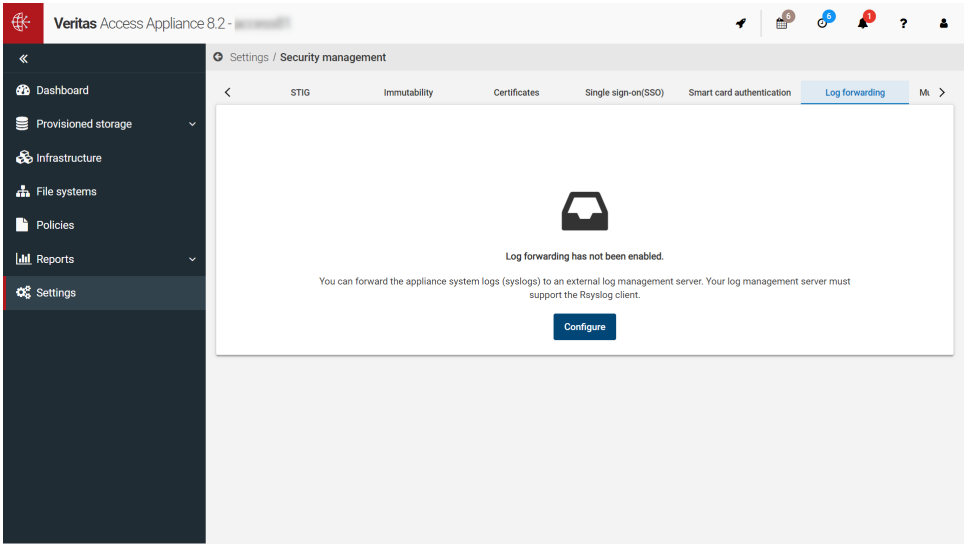
Configuring log forwarding using the UI

You can forward the appliance system logs (syslogs) to an external log management server. Your log management server must support the Rsyslog client.

To configure log forwarding:

1. Sign in to the Access Appliance UI by using the `http://`*`console-ip`*`:14161` URL, where *console-ip* is the management console IP address.
2. Do one of the following:
   - Click **Dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
   - Click **Settings > Security management > Log forwarding**

3 Click **Configure**.



4 Enter the following details:

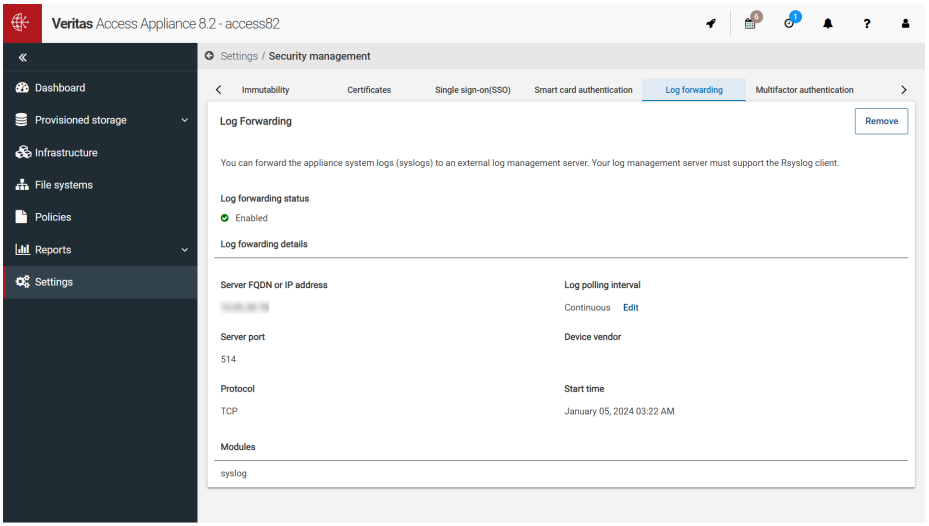
Field	Description
Server FQDN or IP address	FQDN or the IP address of the external log management server.
Server port	Port number of the external log management server. Default port is 514. You can specify a different port if the log server is configured to listen on that port.
Protocol	Select either UDP or TCP. TCP is the default protocol. With TCP protocol, you can optionally enable TLS log transmission. **Note:** Enabling TLS requires that you upload certificates obtained from CA authority and a private key to the appliance.
Log polling interval	Duration in minutes after which the log server polls for the system logs. Logs on the remote log server will be available after that duration. Set the interval in minutes. The options are **15**, **30**, **45**, **60**, **Continuous**. If you select **Continuous**, the appliance continuously forwards logs to the log server.
Device vendor	Unique name for the external log server. You can use any name to identify to which server the appliance is forwarding the logs to.

Field	Description
Enable TLS log transmission	If you want to secure the transmission of logs from the appliance to the log server, select **Enable TLS log transmission** and upload the required certificate files. Veritas recommends that you enable TLS for security purposes. This option provides end-to-end security of data sent over the network from the appliance to the log server. You need a CA certificate and the client private key to configure TLS log transmission. This option is available only if you select the TCP protocol. If you enable secure log transmission, upload CA certificate (X.509 certificate for the certificate authority in PEM format), client certificate (X.509 certificate for the appliance to communicate with the log management server, in PEM format), and client certificate key (RSA key of the client certificate) onto your log server and then upload the certificates to the appliance.

Field	Description
Modules	Types of logs that are forwarded to the log server. Only the OS logs are forwarded and the **syslog** option is selected by default.

5 Click **Enable**.

A notification about the task is displayed on the top of the page. To monitor the progress, click **View details**. After the configuration is completed successfully, a notification is displayed on top of the page. The log forwarding status is shown **Enabled** and the start time for forwarding the logs is displayed.



See “Forwarding logs to an external server” on page 308.

See “Removing log forwarding using the UI” on page 313.

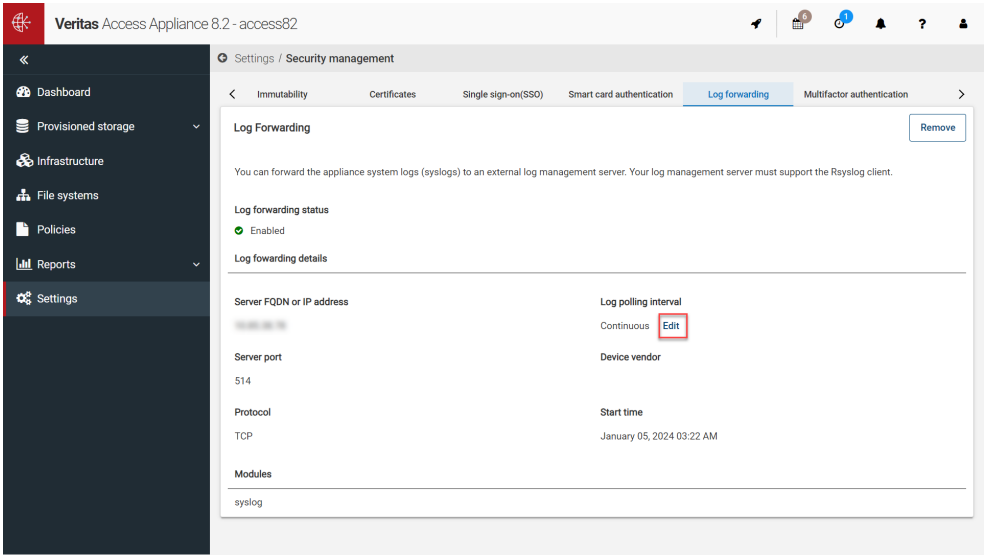
See “Modifying log forwarding settings using the UI” on page 312.

Modifying log forwarding settings using the UI

You can edit only the scheduled interval for forwarding the logs. To edit any other settings, delete the configured log server settings and reconfigure log forwarding.

To edit the settings:

1. Sign in to the Access Appliance UI by using the `http://console-ip:14161` URL, where *console-ip* is the management console IP address.
2. Do one of the following:
   - Click **Dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
   - Click **Settings > Security management > Log forwarding**
3. Under **Log polling interval**, click **Edit**.



4. Select the time interval and click **Save**.

   A notification is displayed on the top of the page. To monitor the progress, click **View details**. After the task is completed successfully a notification is displayed on the top of the page and the changed interval is displayed in the UI.

Removing log forwarding using the UI

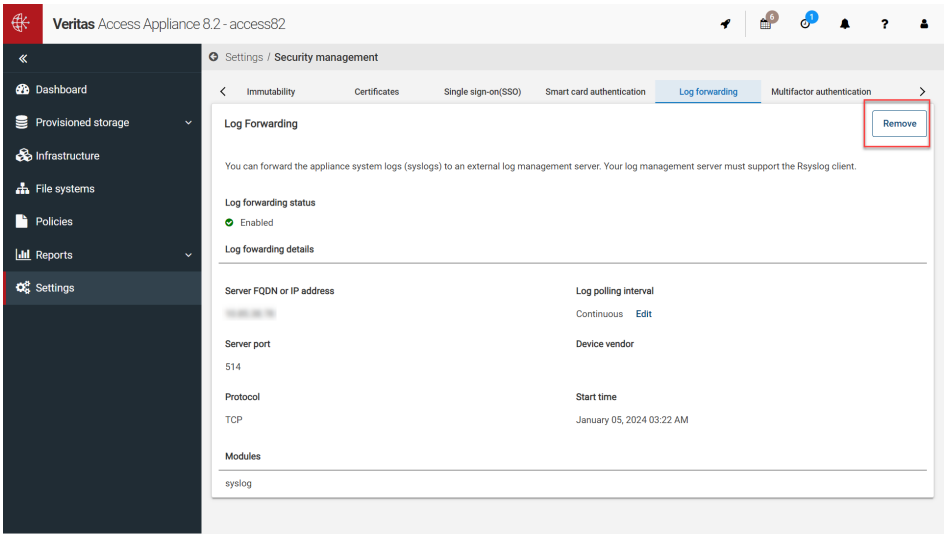
To stop forwarding logs:

1. Sign in to the Access Appliance UI by using the `http://console-ip:14161` URL, where *console-ip* is the management console IP address.
2. Do one of the following:

- Click **Dashboard > Security Meter > View details > Auditing and alerting > Log forwarding**
- Click **Settings > Security management > Log forwarding**

3 Click **Remove**.

A notification is displayed on the top of the page. To monitor the progress, click **View details**.



Setting up log forwarding using the command-line interface

You can use the Cohesity NetBackup command-line interface to set up log forwarding. Use the `Report> syslog` commands on the NetBackup command-line interface to set up the log forwarding. For more details, see the *Veritas Access Command Reference Guide*.

Viewing the configured settings from the appliance shell menu

You can view the configured settings for an appliance node by using the `show log-forwarding` command. The following details are displayed:

- IP address of the log management server.
- Port number of the log management server.
- Protocol used for forwarding the logs to the log management server.

- Time interval in minutes for forwarding logs. The options are 0, 15, 30, 45, or 60. The default is 60. If the interval is set to 0, appliance continuously forwards syslogs to the log management server.
- Whether TLS is enabled for secure log transmission.

For more details, see the *Veritas Access Appliance Command Reference Guide*.