

NetBackup™ Self Service Release Notes

Release: 11.2

NetBackup™ Self Service Release Notes

Last updated: 2026-09-15

Legal Notice

Copyright © 2026 Cohesity Inc All rights reserved.

© 2026 Cohesity Inc All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity Inc in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

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

Support/Service Assistance

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

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

Cohesity Software Running on Partner Hardware

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

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

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

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

Contents

Chapter 1	NetBackup Self Service Release Notes	5
	About NetBackup Self Service 11.2	5
Chapter 2	New features & enhancements - 11.2	7
	New features and enhancements	7
	Known issues	10
	Bugs fixed	12
	Upgrade from previous versions	13

NetBackup Self Service Release Notes

This chapter includes the following topics:

- [About NetBackup Self Service 11.2](#)

About NetBackup Self Service 11.2

NetBackup Self Service 11.2 empowers users to self-serve common backup and restore requests while providing automation and control to IT.

Self Service's multi-tenant, role-based access, and dashboard features provide visibility over what's protected and ongoing backup usage. Self Service's request forms put complex policy management tasks safely in the hands of users who are not trained in the complexities of NetBackup administration.

For Enterprises

Managing backups and restores for many thousands of endpoints across multiple locations and data centers is a task that typically requires a team of specialists. Effecting changes to policies can be a time consuming, error prone, manual activity that can leave vital resources unprotected.

Enabling an intuitive self-service portal reduces complexity and errors, and automates a significant number of manual policy change activities. It also enables non-backup specialists to carry out backup and recovery-related tasks in a controlled and audited environment.

For Service providers

Providing backup and restore services to multiple tenants across mixed platforms is a challenge for many service providers. Service providers can enable self-service

and automate tenant requests for backups and restores. This action puts the tenant in control and significantly reduces provisioning costs.

NetBackup Self Service allows multiple tenants to access a tailored, self-service portal through which requests to back up and restore infrastructure are made intuitively. The status of their protected environments is tracked and reported.

Service providers gain from automation while ensuring strict separation and security between tenant environments. Tenants gain control and visibility over what is protected.

Installation

For details of how to install NetBackup Self Service, please refer to the *NetBackup Self Service 11.2 Installation Guide*.

New features & enhancements - 11.2

This chapter includes the following topics:

- [New features and enhancements](#)
- [Known issues](#)
- [Bugs fixed](#)
- [Upgrade from previous versions](#)

New features and enhancements

Installation and configuration updates

Starting in 11.2, connection strings and machine secrets are stored in `{ProgramFolder}\Config\` instead of in each service-specific `appsettings.json` file.

- `{ProgramFolder}\Config\connectionStrings.json` stores database connection strings and can be encrypted at rest.
- `{ProgramFolder}\Config\machine.secrets.enc` stores DPAPI-protected secrets, including the `ApplicationKey`.
- Service-specific `appsettings.json` files under `Website`, `Api`, `DirectaService`, and `WebService` no longer store connection strings after installation or upgrade.

After each production installation or upgrade, run `nsscmd.exe -getconfig` and store the output in a password vault or secure runbook. The `ApplicationKey` is required for disaster recovery, load-balanced server setup, and fresh installation against an existing database.

ApplicationKey preservation on upgrade

Upgrade preserves the installed ApplicationKey from the central configuration folder or supported legacy sources. Re-running upgrade with a different key in a staging file does not rotate the production key.

If the installation directory changes, upgrade copies the central `Config` folder from the old program folder to the new folder before database steps. The source `Config` folder is removed only after upgrade completes successfully.

Configurator improvements

- The upgrade pre-check now reads database connection information from `{ProgramFolder}\Config\` when `Website\appsettings.json` no longer contains connection strings.
- For a fresh installation that uses an existing database, the Configurator validates the ApplicationKey from the previous installation and writes it to `Install.ini`. Manual `Install.ini` updates are not required when you use the GUI.
- For a fresh installation that creates new databases, main and adapter database credentials are generated automatically.

Uninstall and reinstall hardening

`UnInstall.bat` keeps `{ProgramFolder}\Config\` for disaster recovery. During reinstall, 11.2 handles leftover configuration as follows:

- For a fresh installation with a new database, leftover Config data is removed before a new ApplicationKey is generated.
- For reinstall with an existing database, Config data is kept when the ApplicationKey matches the database and removed when the key does not match.

Silent installer deprecation

Starting in 11.2, `SilentInstall.bat` and `SilentUpgrade.bat` are deprecated. Use the Configurator GUI for installation and upgrade. Command-line installation remains supported by editing `Install Files\Install.ini` and running `Install Files\Install.bat` as an administrator.

Security updates

- CSRF protection is enabled on relevant forms.
- Disabled Windows accounts can no longer sign in to NSS.
- JWT signing keys and machine secrets are protected with DPAPI.

- The command `nsscmd.exe -setsecret` blocks ApplicationKey rotation after the initial configuration.

Kubernetes and Nutanix Support Enhancement NSS 11.2

As part of the NSS 11.2 release, support has been added for Kubernetes and Nutanix within the existing VMware protection workflow.

This enhancement introduces a unified protection model where Kubernetes and Nutanix workloads now use the NetBackup policy template framework, similar to the existing VMware implementation. The previous protection logic for Kubernetes and Nutanix has been re-architected to align with the VMware workflow and reuse the same underlying logic.

With this change:

Protection plans created for Kubernetes and Nutanix workloads must use NetBackup policy templates, following the same approach currently used for VMware protection. NetBackup has been updated across all required components to support policy template integration for protecting Kubernetes pods and Nutanix clusters. The workflow provides consistency across VMware, Kubernetes, and Nutanix workload protection and simplifies protection plan management.

This enhancement standardizes workload protection by adopting a common policy-based architecture across supported platforms.

SQL Server workload usage not calculated

SQL Server workload usage is now calculated and reflected in NetBackup Self Service usage metrics.

Email template customization

Template changes made in Settings → Email Templates are now saved to the database. If you customized templates in 11.1 or earlier (XML under `Website\EmailTemplates`), back up those XML files before upgrade, then after upgrading to 11.2, re-enter each template in the customization screen and click **Save** once to store them in the database.

See the Configuration Guide for details.

Dark mode

A theme toggle in the header lets users switch between light and dark UI. The choice is remembered per browser.

Security

CSRF protection added on relevant forms; disabled Windows accounts can no longer sign in to NSS

Branding / paths

Uploaded images use Cohesity storage path instead of Veritas

Kubernetes and Nutanix Protection Workflow Changes

Starting in release 11.2, Kubernetes and Nutanix workloads are protected using NSS policy templates, the same policy-based model used for VMware.

Impact

- Kubernetes and Nutanix assets protected in releases earlier than 11.2 are not compatible with the new policy-based workflow.
- After upgrading to release 11.2 or later, existing legacy protections and backup images for these workloads cannot be used for restore operations.
- The legacy protection method is no longer supported in release 11.2 and later.

Required action

Re-protect Kubernetes and Nutanix assets by using the appropriate NSS policy template after upgrading. If legacy Kubernetes or Nutanix assets are still in use, plan their migration and re-protection before upgrading to release 11.2 or later.

Known issues

Note the following issues:

Installation and upgrade UI display

The installation and upgrade screens might not display correctly on systems with lower display resolutions.

Workaround: Use a screen resolution of 1920 × 1020 or higher for the best experience.

Upgrade from a fresh installation using an existing database

Upgrading to version 11.1 from a fresh installation that uses an existing database is not supported. During uninstallation, version 11.1 removes files that are required for the upgrade process.

Workaround: None.

Note: Starting with version 11.2, the uninstallation process preserves the required files. As a result, upgrading from a fresh 11.2 installation using an existing database is supported in subsequent releases.

Tenant-specific capacity reporting with the Use Data Transferred Values setting

Capacity usage calculations can vary between the Admin and Tenant pages when the **Use Data Transferred Values** setting is configured differently at the global and tenant levels.

Details:

- When the setting is enabled globally, consumed capacity is calculated using **TransferredSizeBytes** and displayed on both the Admin and Tenant pages.
- When the setting is configured at the tenant level, consumed capacity is calculated using **TransferredSizeBytes** and displayed only on the Tenant page. Different tenants can display different usage values based on their individual settings.

Usage data calculations might not update completely

In some environments, usage calculations might not update all usage data correctly.

Workaround: Restart the Windows service and then perform a system synchronization.

Status: The issue is under investigation. A fix might be provided in a future patch release.

Database connection strings missing encryption attributes after upgrade

When upgrading to NetBackup Self Service 11.2, the installer copies existing database connection strings from earlier NetBackup Self Service versions. If the source NetBackup Self Service version is earlier than 10.5.0.1, the existing connection strings in `appsettings.json` might not include the following required attributes:

`;Encrypt=false;TrustServerCertificate=true`

These attributes were introduced after NetBackup Self Service 10.3.0.1 because of changes to SQL Server database encryption requirements. During the upgrade, the installer copies the existing connection strings without modifying them. As a result, the required attributes might be missing after the upgrade.

Affected Configurations:

- NetBackup Self Service versions earlier than 10.5.0.1.
- Upgrades to NetBackup Self Service 11.2.
- Existing connection strings that do not contain:
`;Encrypt=false;TrustServerCertificate=true`

Workaround:

To apply the workaround

- 1 Open the following file: `{ProgramFolder}/Config/connectionstrings.json`.
- 2 Verify that the MainDB and AdapterDb connection strings contain the following attributes: **`;Encrypt=false;TrustServerCertificate=true`**.
- 3 If the attributes are missing, append the following string to the end of both connection strings, before the closing quotation mark:
`;Encrypt=false;TrustServerCertificate=true`.
- 4 Save the file.
- 5 Restart the Self Service Windows service and IIS.
- 6 Verify that:
 - The website is accessible.
 - The Self Service Windows service is running.
 - The service does not terminate unexpectedly.

Known installer limitations

Table 2-1 Installer limitations

Limitation	Status	Workaround
DAPI password in <code>connectionStrings.json</code>	Uses ChangeMe after fresh installation	Configure DAPI after installation.
ApplicationKey rotation	Not supported after initial configuration	Restore the ApplicationKey from backup.
Copying <code>machine.secrets.enc</code> between nodes	Not supported because the file is DPAPI-protected	Use the same ApplicationKey value on each node.
Partial InitData retry	Not automated	Restore the database and retry from a clean state.

Bugs fixed

- **SQL Server workload usage not calculated:** SQL Server workload usage is currently not calculated or reflected in NetBackup Self Service usage metrics.
- **Expired images:** Status display corrected for expired images.
- **Installer reliability updates:**

- InitData writes sqlcmd output to a temporary file to reduce memory pressure.
- Install SQL scripts are read as UTF-8.
- InitData failures are logged instead of being silently masked.

Upgrade from previous versions

For load-balanced NetBackup Self Service installations, synchronize the central `Config` folder settings across all web servers after an upgrade. Do not copy the `machine.secrets.enc` file between servers, as this method is not supported. Instead, use the commands: `nsscmd -getconfig`, `nsscmd -setconfig`, and `nsscmd -setsecret` as described in the *NetBackup Self Service Installation Guide*.

If you currently use SQL Server 2016 or later, you can upgrade to this version of NetBackup Self Service from the following earlier versions: All versions from 7.7 through 10.34.

For more compatibility details, see the NetBackup Software Compatibility List.

Silent Install and Upgrade has been deprecated as of version 11.2, however the `Download Prerequisites.bat` and `Install Prerequisites.bat` files are still available in the `install` folder for installs where the NSS server itself is not connected to the internet or BITS is disabled on the NSS machine. In that case the `Download Prerequisites.bat` file can help download the NSS prerequisites to a 'Prerequisites' folder on another machine and then these can be copied to the NSS machine along with `Install Prerequisites.bat` to install them to the NSS machine.

You can find further information in the *NetBackup Self Service Installation Guide*. Read the "Prerequisites" section carefully to ensure that your environment can support NetBackup Self Service 11.2.

Upgrade Considerations (Release 11.2)

Warning: Important: Release 11.2 introduces installer changes that affect the storage location of connection strings and application keys.

Before upgrading, take a snapshot of the virtual machine (VM) or back up the `appsettings.json` files from the following directories:

- Directories containing `appsettings.json` files:
 - `/Api`
 - `/DirectaService`
 - `/WebService`

- /WebSite

Review the Installation Guide carefully, as these changes take effect starting with release 11.2.

When upgrading from a version earlier than 11.2, run the 11.2 installer directly without uninstalling the existing installation.

The installer automatically detects and performs an upgrade when a previous version is present. Uninstalling the existing version before upgrading is not recommended.

Impact: Backing up configuration files before upgrading helps ensure that you can revert to the previous version if the upgrade does not complete successfully.