SPECTRA STORCYCLE SOLUTION

USER GUIDE

www.SpectraLogic.com

Legal Notices

Copyright

Copyright © 2019 - 2024 Spectra Logic Corporation. All rights reserved. This item and the information contained herein are the property of Spectra Logic Corporation.

Notices

Except as expressly stated herein, Spectra Logic Corporation makes its products and associated documentation on an "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, BOTH OF WHICH ARE EXPRESSLY DISCLAIMED. In no event shall Spectra Logic be liable for any loss of profits, loss of business, loss of use or data, interruption of business, or for indirect, special, incidental or consequential damages of any kind, even if Spectra Logic has been advised of the possibility of such damages arising from any defect or error.

Information furnished in this manual is believed to be accurate and reliable. However, no responsibility is assumed by Spectra Logic for its use. Due to continuing research and development, Spectra Logic may revise this publication from time to time without notice, and reserves the right to change any product specification at any time without notice.

Trademarks

Attack Hardened, BlackPearl, BlueScale, RioBroker, Spectra, SpectraGuard, Spectra Logic, Spectra Vail, StorCycle, TeraPack, TFinity, and TranScale are registered trademarks of Spectra Logic Corporation. All rights reserved worldwide. All other trademarks and registered trademarks are the property of their respective owners.

Part Number

90990140 Revision O

Revision History

Revision	Date	Description
K	April 2023	Updated for StorCycle 4.0.0.
L	November 2023	Updated for StorCycle 4.1.0.
M	December 2023	Updated for StorCycle 4.1.1.
N	February 2024	Updated for StorCycle 4.2.0.
O	October 2024	Updated for StorCycle 4.3.0

Note: To make sure you have the release notes for the most current version of the StorCycle Release Notes, check the Spectra Logic Technical Support portal at *support.spectralogic.com/documentation/release-notes/*.

To make sure you have the most current version of this guide check the Spectra Logic Technical Support portal at *support.spectralogic.com/documentation/user-guides/*.

Master License Agreement

This Master License Agreement governs use of Spectra Logic Corporation stand-alone software such as StorCycle software ("Software"). Your organization has agreed to the license contained herein and terms and conditions of this Master License Agreement (the "MLA"). Use of the Software is affirmation of your acceptance and grants to your organization ("Licensee") the right to use the Software.

1. License.

1.1 Grant of License. Subject to all of the terms and conditions of this MLA, Spectra Logic Corporation and its wholly-owned subsidiaries ("Spectra") grant to Licensee a non-transferable, non-sublicensable, non-exclusive license during the applicable Term (as defined below) to use the object code form of the Software specified in the quote supplied either by Spectra or an authorized reseller internally and for operational use, and only in accordance with the technical specification documentation generally made available by Spectra to its licensees with regard to the Software ("Documentation"). The term "Software" will include any Documentation and any ordered Support and maintenance releases of the same specific Software product provided to Licensee under this MLA.

1.2 Term and Renewals. The Software is licensed under a subscription basis or is permanently licensed, as defined herein. Licensee's Software license is stated on the quote provided to Licensee.

(a) If the Software is ordered on a subscription basis ("Subscription"), the term of the software license will (i) commence upon receipt of a purchase order issued to Spectra directly from Licensee or from an authorized reseller issued on your behalf and will (ii) continue for the number of year(s) noted on the quote commencing on the date of activation of key(s) performed by Spectra Professional Services ("Subscription Term"). Unless terminated earlier in accordance with section 4, each Software Subscription Term will automatically renew upon expiration of the initial Software Subscription Term for additional successive terms unless either party gives the other prior written notice of cancellation at least thirty (30) days prior to expiration of the then-current term. Unless otherwise specified on the quote, the license fee for any Software Subscription Term renewal will be based on the then-current Subscription rates.

(b) If the Software is ordered on a permanent license basis ("Permanent"), the term of the software license will not expire except in accordance with section 4. The term of associated products such as support, user, server and storage elections will commence upon on the date of activation of key(s) performed by Spectra Professional Services and may be renewed at such time as the term of such quoted election(s) expire.

1.3 Installation. Software may be installed on Licensee's computers only by Licensee's employees, authorized resellers, or by Spectra Professional Services as requested by Licensee.

1.4 License Restrictions. Licensee shall not (and shall not allow any third party) to

(a) decompile, disassemble, or otherwise reverse engineer the Software or attempt to reconstruct or discover any source code, underlying ideas, algorithms, file formats or programming interfaces of the Software by any means whatsoever (except and only to the extent that applicable law prohibits or restricts reverse engineering restrictions, and then only with prior written notice to Spectra), (b) distribute, sell, sublicense, rent, lease or use the Software (or any portion thereof) for time sharing, hosting, service provider or like purposes, (c) remove any product identification, proprietary, copyright or other notices contained in the Software, (d) modify any part of the Software, create a derivative work of any part of the Software, or incorporate the Software into or with other software, except to the extent expressly authorized in writing by Spectra, or (e) publicly disseminate Software performance information or analysis (including, without limitation, benchmarks).

2. Ownership.

Notwithstanding anything to the contrary contained herein, except for the limited license rights expressly provided herein, Spectra retains all rights, title and interest in and to the Software (including, without limitation, all patent, copyright, trademark, trade secret and other intellectual property rights) and all copies, modifications and derivative works thereof. Licensee acknowledges that it is obtaining only a limited license right to the Software and that irrespective of any use of the words "purchase", "sale" or like terms hereunder no ownership rights are being conveyed to Licensee under this MLA or otherwise.

3. Payment and Delivery.

3.1 Payment. All payments, either to Spectra or an authorized reseller, are non-refundable (except as expressly set forth in this MLA). Unless otherwise specified on the applicable quote, all license fees, support and Professional Services fees, if any, are due within thirty (30) days of date of invoice. Licensee shall be responsible for all taxes, withholdings, duties and levies arising from the order (excluding taxes based on the net income of Spectra). Any late payments shall be subject to a service charge equal to 1.5% per month of the amount due or the maximum amount allowed by law, whichever is less.

3.2 Delivery. Immediately upon receipt of a purchase order from Licensee or on behalf of Licensee or from an authorized reseller on behalf of Licensee, Licensee will have the right to access the Software. Software will be delivered by electronic means unless otherwise specified on the applicable quote. Spectra will contact Licensee and request its server identification number(s) and provide Activation code(s).

4. Term of MLA.

4.1 Term.

(a)(i) If Licensee ordered a Software Subscription License, this MLA expires on the day the Term of the Software expires. However, the ability to retrieve/restore archived data will continue indefinitely.

(ii) If a Permanent Software License was ordered, the software license does not expire.

(b) Section 4.1(a) is subordinate to this section 4.1(b). Either party may terminate this MLA if the other party (a) fails to cure any material breach of this MLA within thirty (30) days after written notice of such breach, (b) ceases operation without a successor; or (c) seeks protection under any bankruptcy, receivership, trust deed, creditors arrangement, composition or comparable proceeding, or if any such proceeding is instituted against such party (and not dismissed within sixty (60) days thereafter). Termination is not an exclusive remedy and the exercise by either party of any remedy under this MLA will be without prejudice to any other remedies it may have under this MLA, by law, or otherwise.

4.2 Survival. Sections 1.4 (License Restrictions), 2 (Ownership), 3 (Payment and Delivery), 4 (Term of MLA), 5.3 (Disclaimer), 8 (Limitation of Remedies and Damages), 10 (Confidential Information), 11 (General), and Licensee's right to Work Product and ownership of Licensee Content described in Section 7 shall survive any termination or expiration of this MLA.

5. Limited Warranty and Disclaimer.

5.1 Limited Warranty. Spectra warrants to Licensee that for a period of ninety (90) days from the effective date (the "Warranty Period"), the Software shall operate in substantial conformity with the Documentation. In addition, Spectra warrants that (i) it has the right to enter into and perform all obligations under this MLA, (ii) no agreement exists that restricts or conflicts with the performance of Spectra's rights and obligation hereunder, (ii) the technical information provided to Licensee is accurate and complete, and (iv) the Software is free from any third-party intellectual property infringement claims. Spectra does not warrant that Licensee's use of the Software will be uninterrupted or error-free, will not result in data loss, or that any security mechanisms implemented by the Software will not have inherent limitations. Spectra's sole liability (and Licensee's exclusive remedy) for any breach of this warranty shall be, in Spectra's sole discretion, to use commercially reasonable efforts to provide Licensee with an error-correction or work-around which corrects the reported non-conformity, to replace the non-conforming Software with conforming Software, or if Spectra determines such remedies to be impracticable within a reasonable period of time, to terminate the Software license and refund the license fee and support fee, if any, paid for the non-conforming Software. Spectra shall have no obligation with respect to a warranty claim unless notified of such claim within the Warranty Period.

5.2 Exclusions. The above warranty will not apply (a) if the Software is used with hardware or software not specified in the Documentation, (b) if any modifications are made to the Software by Licensee or any third party, (c) to defects in the Software due to accident, abuse or improper use by Licensee, or (d) to items provided on a no charge or evaluation basis.

5.3 Disclaimer. THIS SECTION 5 CONTAINS A LIMITED WARRANTY AND EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 5 THE SOFTWARE AND ALL SERVICES ARE PROVIDED "AS IS". NEITHER SPECTRA NOR ANY OF ITS SUPPLIERS MAKES ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. LICENSEE MAY HAVE OTHER STATUTORY RIGHTS. HOWEVER, TO THE FULL EXTENT PERMITTED BY LAW, THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE LIMITED WARRANTY PERIOD.

6. Support.

Spectra will provide the support services identified in the quote ("Support"). Support services for the Subscription License will coincide with the license term.

7. Professional Services.

7.1 Professional Services. Professional Services may be ordered by Licensee pursuant to a quote describing the work to be performed, fees and any applicable milestones, dependencies and other technical specifications or related information. The parties acknowledge that the scope of the Professional Services provided hereunder consists solely of either or both of (a) assistance with Software installation, deployment, and usage or (b) development or delivery of additional related Spectra copyrighted software or code. Spectra shall retain all right, title and interest in and to any such work product, code or software and any derivative, enhancement or modification thereof created by Spectra (or its agents) ("Work Product").

7.2 Licensee Content. Licensee grants Spectra a limited right to use any Licensee materials provided to Spectra in connection with the Professional Services (the "Licensee Content") solely for the purpose of performing the Professional Services for Licensee. Licensee owns and will retain ownership (including all intellectual property rights) in the Licensee Content.

8. Limitation of Remedies and Damages.

8.1 NEITHER PARTY SHALL BE LIABLE FOR ANY LOSS OF USE, LOST DATA, FAILURE OF SECURITY MECHANISMS, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS), REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

8.2 NOTWITHSTANDING ANY OTHER PROVISION OF THIS MLA, SPECTRA'S AND AUTHORIZED RESELLER'S, IF ANY, ENTIRE LIABILITY TO LICENSEE SHALL NOT EXCEED THE AMOUNT ACTUALLY PAID BY LICENSEE UNDER THIS MLA.

8.3 THIS SECTION 8 SHALL NOT APPLY WITH RESPECT TO ANY CLAIM ARISING UNDER THE SECTIONS TITLED "GRANT OF LICENSE," "LICENSE RESTRICTIONS" OR "CONFIDENTIAL INFORMATION."

9. Indemnification.

(a) Spectra shall defend, indemnify and hold harmless Licensee from and against any claim of infringement of a patent, copyright, or trademark asserted against Licensee by a third party based upon Licensee's use of the Software in accordance with the terms of this MLA, provided that Spectra shall have received from Licensee (i) prompt written notice of such claim (but in any event notice in sufficient time for Spectra to respond without prejudice), (ii) the exclusive right to control and direct the investigation, defense, and settlement (if applicable) of such claim, and (iii) all reasonably necessary cooperation of Licensee.

(b) If Licensee's use of any of the Software is, or in Spectra's opinion is likely to be, enjoined due to the type of infringement specified above, or if required by settlement, Spectra may, in its sole discretion (i) substitute for the Software substantially functionally similar programs and documentation, (ii) procure for Licensee the right to continue using the Software, or if (i) and (ii) are commercially impracticable, (iii) terminate the MLA and refund to Licensee the license fee.

(c) The foregoing indemnification obligation of Spectra shall not apply if the Software is modified by any person other than Spectra, but solely to the extent the alleged infringement is caused by such modification, if the Software is combined with other non-Spectra products or process not authorized by Spectra, but solely to the extent the alleged infringement is caused by such combination, to any unauthorized use of the Software, to any unsupported release of the Software, or to any open source software or other third-party code contained within the Software. THIS SECTION 9 SETS FORTH SPECTRA'S AND RESELLER'S, IF ANY, SOLE LIABILITY AND LICENSEE'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

10. Confidential Information.

Each party agrees that all code, inventions, know-how, business, technical and financial information it obtains ("Receiving Party") from the disclosing party ("Disclosing Party") constitute the confidential property of the Disclosing Party ("Confidential Information"), provided that it is identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be Confidential Information due to the nature of the information disclosed and the circumstances surrounding the disclosure. Any software, documentation or technical information provided by Spectra (or its agents), performance information relating to the Software, and the terms of this MLA shall be deemed Confidential Information of Spectra without any marking or further designation. Except as expressly authorized herein, the Receiving Party will hold in confidence and not use or disclose any Confidential Information except as necessary to carry out the purpose of this MLA. The Receiving Party's nondisclosure obligation shall not apply to information which the Receiving Party can document (a) was rightfully in its possession or known to it prior to receipt of the Confidential Information, (b) is or has become public knowledge through no fault of the Receiving Party, (c) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation, (d) is independently developed by employees of the Receiving Party who had no access to such information, or (e) is required to be disclosed pursuant to a regulation, law or court order (but only to the minimum extent required to comply with such regulation or order and with advance notice to the Disclosing Party). The Receiving Party acknowledges that disclosure of Confidential Information would cause substantial harm for which damages alone would not be a sufficient remedy, and therefore that upon any such disclosure by the Receiving Party the Disclosing Party shall be entitled to appropriate equitable relief in addition to whatever other remedies it might have at law.

11. General.

11.1 Assignment. This MLA will bind and inure to the benefit of each party's permitted successors and assigns. Neither party shall assign this MLA (or any part thereof) without the advance written consent of the other party, except that either party may assign this MLA in connection with a merger, reorganization, acquisition or other transfer of all or substantially all of such party's assets or voting securities. Any attempt to transfer or assign this MLA except as expressly authorized under this section 11.1 is null and void.

11.2 Severability. If any provision of this MLA shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited to the minimum extent necessary so that this MLA shall otherwise remain in effect.

11.3 Governing Law; Jurisdiction and Venue. This MLA shall be governed by the laws of the State of Colorado and the United States without regard to conflicts of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods. Except where statutory laws prohibit Licensee from entering into arbitration or choice of laws, any dispute or claim relating in any way to Licensee's use of the Software, or of a copyright issue, or to any associated support services, will be resolved by binding arbitration in Denver, Colorado. The prevailing party in any action to enforce this MLA will be entitled to recover its attorneys' fees and costs in connection with such action.

11.4 Amendments; Waivers. No supplement, modification, or amendment of this MLA shall be binding, unless executed in writing by an authorized representative of both parties. No waiver will be implied from conduct or failure to enforce or exercise rights under this MLA. No provision of any purchase order or other business form employed by Licensee will supersede the terms and conditions of this MLA, and any such document relating to this MLA shall be for administrative purposes only and shall have no legal effect.

11.5 Force Majeure. Neither party shall be liable to the other for any delay or failure to perform any obligation under this MLA (except for a failure to pay fees) if the delay or failure is due to events which are beyond the reasonable control of such party, including but not limited to any strike, blockade, war, act of terrorism, riot, natural disaster, failure or diminishment of power or of telecommunications or data networks or services, or refusal of approval or a license by a government agency.

11.6 Export Compliance. Licensee acknowledges that the Software is subject to export restrictions by the United States government and import restrictions by certain foreign governments. Licensee shall not and shall not allow any third-party to remove or export from the United States or allow the export or re-export of any part of the Software or any direct product thereof (a) into (or to a national or resident of) any embargoed or terrorist-supporting country, (b) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals, (c) to any country to which such export or re-export is restricted or prohibited, or as to which the United States government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval, or (d) otherwise in violation of any export or import restrictions, laws or regulations of any United States or foreign agency or authority. Licensee agrees to the foregoing and warrants that it is not located in, under the control of, or a national or resident of any such prohibited country or on any such prohibited party list. The Software is further restricted from being used for the design or development of nuclear, chemical, or biological weapons or missile technology, or for terrorist activity, without the prior permission of the United States government.

11.7 Third-Party Code. The Software may contain or be provided with components subject to the terms and conditions of third party "open source" software licenses ("Open Source Software"). Open Source Software may be identified in the Documentation, or Spectra shall provide a list of the Open Source Software for a particular version of the Software to Licensee upon Licensee's written request. To the extent required by the license that accompanies the Open Source Software, the terms of such license will apply in lieu of the terms of this MLA with respect to such Open Source Software.

11.8 Entire Agreement. This MLA is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements and communications relating to the subject matter contained herein.

Amazon Web Services

If Licensee has licensed Software for use in conjunction with Amazon Web Services, such web services will be provided by Amazon in accordance with its standard terms and conditions. SPECTRA MAKES NO WARRANTY REGARDING AMAZON SERVICES AND SUGGESTS THE USE OF AMAZON’S CONTINUOUS DATA BACK UP SERVICES.

CONTACTING SPECTRA LOGIC

To Obtain General Information	
Spectra Logic Website: ***spectralogic.com***	
United States Headquarters	**European Office**
Spectra Logic Corporation 6285 Lookout Road Boulder, CO 80301 USA **Phone:** 1.800.833.1132 or 1.303.449.6400 **International:** 1.303.449.6400	Spectra Logic Europe Ltd. 329 Doncastle Road Bracknell Berks, RG12 8PE United Kingdom **Phone:** 44 (0) 870.112.2150
Spectra Logic Technical Support	
Technical Support Portal: ***support.spectralogic.com***	
United States and Canada **Phone:** **Toll free US and Canada:** 1.800.227.4637 **International:** 1.303.449.0160	**Europe, Middle East, Africa** **Phone:** 44 (0) 870.112.2185 **Deutsch Sprechende Kunden** **Phone:** 49 (0) 6028.9796.507 **Email:** spectralogic@stortrec.de
Mexico, Central and South America, Asia, Australia, and New Zealand **Phone:** 1.303.449.0160	
Spectra Logic Sales	
Website: ***shop.spectralogic.com***	
United States and Canada **Phone:** 1.800.833.1132 or 1.303.449.6400 **Email:** sales@spectralogic.com	**Europe** **Phone:** 44 (0) 870.112.2150 **Email:** eurosales@spectralogic.com
To Obtain Documentation	
Spectra Logic Website: ***support.spectralogic.com/documentations/documentation***	

TABLE OF CONTENTS

Helpful Information

These instructions describe how to configure, use, and monitor the Spectra® StorCycle® Solution, sometimes referred to as the *solution*.

Intended Audience

This guide is intended for data center administrators and operators who maintain and operate file storage systems. The information in this guide assumes a familiarity with computing terminology. You also need to be familiar with installing, configuring, and using data file storage and archival software.

User Interface Screens

The user interface changes as new features are added or other modifications are made between software revisions. Therefore, the screens you see in the user interface may differ from those shown in this guide.

Typographical Conventions

This document uses the following conventions to highlight important information:

WARNING Read text marked by the "Warning" symbol for information you must know to avoid personal injury.

CAUTION Read text marked by the "Caution" symbol for information you must know to avoid losing data.

IMPORTANT Read text marked by the "Important" symbol for information that helps you complete a procedure or avoid extra steps.

Note: Read text marked with "Note" for additional information or suggestions about the current topic.

User Feedback

Contact us at (800) 833-1132 to give us suggestions or feedback on our products and documentation.

Related Publications

The latest revision of the following documents related to the Spectra Spectra StorCycle Solution are available as PDF files on the Spectra Logic® website at: *support.spectralogic.com/documentations/user-guides.*

- The *Spectra StorCycle Solution Getting Started Guide* provides a quick reference for installing and configuring the Spectra StorCycle solution.
- The *Spectra StorCycle Solution User Guide* provides detailed information about installing, configuring, and using the Spectra StorCycle solution. The content of this guide, for your revision of the StorCycle solution, is accessible by clicking **Help** in the toolbar of the software.

The following document is available after logging into your Support portal account at: *support.spectralogic.com*.

- The *Spectra StorCycle Solution Release Notes and Documentation Updates* provide the most up-to-date information about the solution, including information about the latest software releases and documentation updates.

For additional information about the Spectra BlackPearl® Nearline gateway and the Spectra BlackPearl NAS solution, refer to the publications listed in this section.

- The *Spectra BlackPearl Nearline Gateway User Guide* provides detailed information about configuring, using, and maintaining your BlackPearl system.
- The *Spectra S3 API Reference* provides information on understanding and using the Spectra S3 API.
- The *Spectra BlackPearl Eon Browser User Guide* provides installation and usage information for the BlackPearl Eon Browser.
- The *Spectra BlackPearl NAS Solution User Guide* provides information about configuring, using and maintaining your BlackPearl NAS solution.

The following documents are available after logging into your Support portal account at: *support.spectralogic.com*.

- The *Spectra BlackPearl Release Notes and Documentation Updates* provide the most up-to-date information about the BlackPearl and BlackPearl NAS systems, including information about the latest software releases and documentation updates.

API DOCUMENTATION

To access the documentation for the REST API, after StorCycle is installed, go to *https://localhost/apidocs/*.

For the open API yaml file, go to

https://localhost/openapi.yaml

For additional API documentation, examples, and a generated client, go to *https://github.com/SpectraLogic/storcycle_api/*.

Chapter 1 - Product Overview

This section provides an overview of the Spectra StorCycle solution features.

OVERVIEW

The Spectra StorCycle solution provides an easy and affordable means to move inactive data onto lower cost storage, saving not only cost per terabyte, but also management expenses of backup, auditing, and maintenance. The StorCycle solution provides a framework to identify inactive data and move it to a lower-cost perpetual storage tier, ensuring the data is stored safely while making it easily accessible.

The StorCycle solution is built around four main pillars of functionality:

- Identify — Scan primary storage and identify inactive files
- Migrate and Store — Move inactive files to lower-cost storage, called the "Perpetual Storage Tier"
- Long-Term Management — Ensure files remain safe on the Perpetual Storage Tier for long term or forever
- Retrieve — Allow users to easily access and retrieve migrated files

Figure 1 shows the StorCycle solution system component diagram.

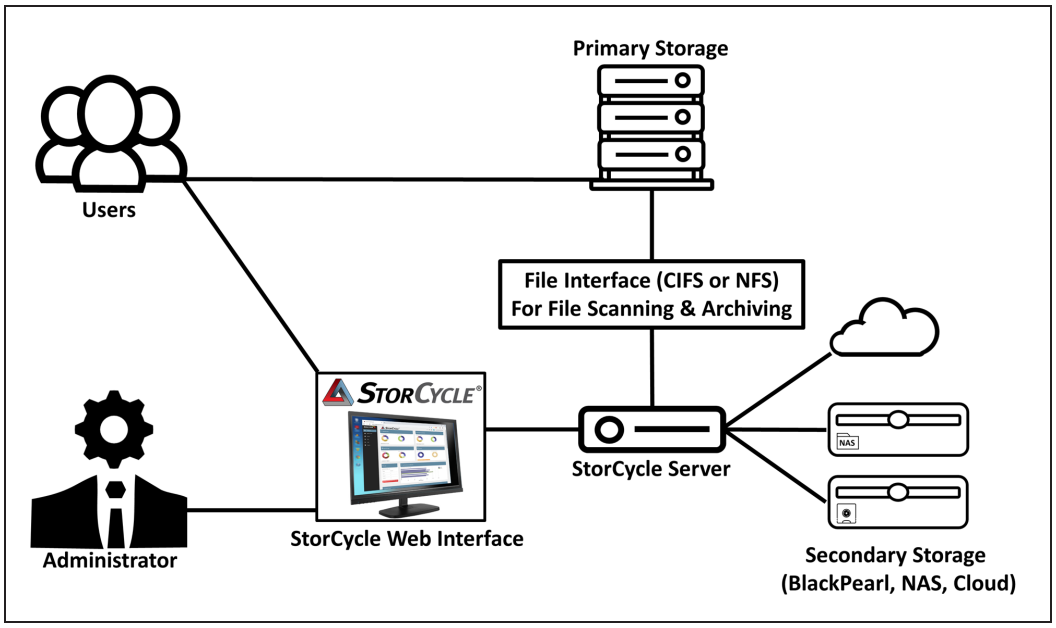


Figure 1 The StorCycle component diagram.

The major physical components of a StorCycle workflow include:

- The organization's existing primary source storage
- The StorCycle server(s)
- Secondary storage target(s)
- An IT Administrator
- A Storage User

The StorCycle server connects to the primary source storage using a CIFS or NFS interface, and to the secondary storage using a CIFS, NFS, S3, Spectra S3, or Microsoft Azure interface. Administrators and users access the StorCycle interface using a web browser. No additional drivers or user software installations are required.

IMPORTANT The StorCycle solution runs on Windows® servers and supports CIFS/SMB networked storage or runs on Linux® servers and supports NFS-protocol storage or CIFS/SMB networked storage.

FEATURES

The Spectra StorCycle solution includes the following features:

Spectra StorCycle User Interface

The user interface can be accessed over an Ethernet network using Google® Chrome™ version 75 or later, on Windows, macOS®, and Linux. It is used to perform configuration and management tasks on the solution and to view system messages.

REST API

It is now possible to interact with the Spectra StorCycle solution using a REST API (application-programming interface). To see the API documentation, go to https://localhost/apidocs/#/ on the StorCycle server.

Multiple Supported Sources

The Spectra StorCycle solution running on a Linux server supports NFS, CIFS/SMB, and S3 sources, and running on a Windows server supports CIFS/SMB and S3 sources.

Multiple Supported Destinations

The Spectra StorCycle solution supports migrating / storing data to multiple destinations including:

- Spectra BlackPearl Converged Storage system
- Spectra BlackPearl NAS solution (NFS and CIFS)
- Non-Spectra NAS (NFS and CIFS)
- S3 Cloud - Files migrated / stored to a standard S3 bucket with tiering to Glacier and Glacier Deep Archive can be restored after the file is tiered.
- Microsoft Azure
- Microsoft Azure Archive

Single Key Encryption

Storage location targets can be configured to have all files encrypted before they are migrated / stored to the target.

Spectra NAS Snapshot Ransomware Protection

Spectra NAS targets can be configured to create a snapshot of the data in a migrate / store job after the job completes. Optionally, targets with snapshots enabled can be set to read-only after migrate / store jobs complete. This provides ransomware protection, but is only suitable for a storage location dedicated to receiving data from StorCycle migrate / store jobs.

Control of Storage Resources and Performance

Spectra and non-Spectra NAS Storage locations can be configured to control peak time versus non-peak time activity.

Transparent Access to Migrated / Stored Files

Files migrated / stored with the **Replacement Option** set to **Remove Source File: create Symbolic link** are replaced with symbolic links which transparently open the replaced files from secondary storage.

Note: To replace migrated / stored files with symbolic links, the migrate / store project must have only one NAS target. Additional BlackPearl or S3 targets are optional.

File Scanning

The Spectra StorCycle solution scans source directories to determine the age and size of files.

Scheduled Scanning, Migrating / Storing, and Restoring

Schedules can be set for scanning, data migration / storing, and restoring projects. Scanning and data migration / storing project can include recurring schedules.

Include and Exclude Filters for Migrating / Storing

For migrate / store projects, the files to include can be filtered by file types to include or exclude, directories to exclude, file sizes to include, and file ages to include. Based on this information, the Migrate / Store wizard determines how much data can be migrated / stored and the resulting cost savings.

File Packing

You can select whether data should be packed into larger files for transfer. The Spectra StorCycle solution features both ZIP and TAR packing protocols.

Migrate / Store Tags

Tags are a way to add metadata to the migrate / store operation. Users can add any number of tags to a migrate / store operation. When restoring data, you can search for the tag to determine from which migrate / store job to restore data.

Retention Policies

Storage Locations can be configured to automatically delete the data migrated / stored by a project after a specified number of days. Users can be configured to receive an email about pending deletions five days before they occur.

Note: Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.

Email Alerts for Completed Restores

When you configure a restore project, you can select to have an email alert sent when the restore job completes.

OpenLDAP Support for Linux Servers

OpenLDAP, an open-source implementation of the Lightweight Directory Access Protocol (LDAP), is used to provide Simple Authentication, Security Layer, and Transport Layer Security.

High Availability Failover on Virtual Machines

The StorCycle solution fully supports the capability of hyper-converged virtual machines (VMs) to provide failover. The VM automatically restarts the StorCycle solution on a new node if one instance fails.

Linked Instances

A StorCycle instance can link to other StorCycle instances to allow searching for data managed by other StorCycle solution installations.

BlackPearl Bucket Ingest

A bucket on a BlackPearl system with data added outside of the StorCycle solution can be ingested so that the objects in the bucket are managed by the StorCycle solution.

BlackPearl Embedded Dashboard

Access the embedded dashboard of configured BlackPearl systems. Users can access and control common features of the BlackPearl system without having to access the BlackPearl user interface.

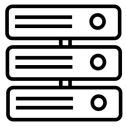
Perpetual Storage

StorCycle offers perpetual storage, which provides lower-cost options compared to primary storage, such as cloud, disk, and tape storage, while ensuring data integrity and safety. StorCycle uses metadata to help administrators identify and migrate inactive data for secondary storage, distribution, backup, archive, and disaster recovery while reducing the load and cost of primary storage.

StorCycle Quick Reference

Use the information in this section to quickly locate information that describes the core functionality and features of the StorCycle solution, as well as workflow examples for typical use case scenarios.

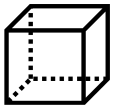
User Role Description **User Roles determine the level of permissions and access within the StorCycle solution**		
	**Administrator**	Administrator has unrestricted access to all storage locations, projects, configuration and reporting.
	**Crypto Officer**	Administrator privileges plus Crypto Officer role. Can configure encryption options and enable the encryption key.
	**Storage Manager**	Users who can create Scan, Migrate / Store, and Restore jobs. • Cannot configure settings or storage locations. • Can restrict access to data with domain integration and group assignments.
	**Restore User**	Domain users who are able to restore data via HTML links from the StorCycle user interface. Administrators can restrict Restore User access to data with domain integration and group assignments.

Storage Locations **Storage Locations are where data will be migrated from and where data will be migrated to.**		
	**Source Storage**	Source data will be scanned and archived. Supported sources include NAS and S3. **Note:** S3 sources can only be migrated to BlackPearl systems, and restore to NAS sources.
	**Target Storage**	Target storage locations where data is archived to. Supported targets include Spectra BlackPearl systems (NAS and Nearline), NAS, S3, AWS, AWS Glacier, and MS Azure.

Projects and Jobs **Each time a Project (Migrate / Store, Scan, or Restore) runs, it creates a job increment. Migrate / Store and Scan jobs can be manually started or set to run on a schedule. Restores can be manually started or set to run at a future date.**		
	**Migrate / Store Project**	• A Migrate / Store Project is configured to move data from a source to one or many targets. • Migrate / Store projects can be configured with a reoccurring schedule. • Age and Size filters can be applied to a Project. • Each time a Migrate / Store project runs, it creates a Migrate / Store Job (MigrateJob-1, MigrateJob-2, etc.).
	**Scan Project**	• A Scan Project is configured to scan source storage locations. • Scan Projects can be configured with a recurring schedule. • Each time a Scan Project runs, it will create a Scan Job (ScanJob-1, ScanJob-2, etc).
	**Restore Project**	• A Restore Project is configured to restore a specific Migrate / Store Job. • Restore projects can be configured to run now or run at a future date or time.
	**Job**	• Jobs refer to any Migrate / Store, Restore, or Scan project / job, as well as other job types, including Retention Policy Delete, Version Delete, Bucket Ingest, and Database Backup. • Every Job is an instance of a running project.

StorCycle Features			
Features		**Description**	**Applies To**
	**AD/LDAP Server**	If enabled, allows users to login to StorCycle using their domain credentials. Required if using Restore Users. AD/LDAP configurations are also used to query the domain to determine Domain Group membership.	Users

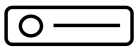
StorCycle Features			
Features		**Description**	**Applies To**
	**Domain Groups**	A single domain group can be assigned to Source storage locations and restrict domain users by group membership. Domain groups are independent of domain file permissions and are only used to prevent or allow access to StorCycle jobs.	Sources and Users
	**Departments**	Departments can be assigned to Source and Target Storage locations and be used to track cost and storage savings. Departments have no relation to users.	Sources and Targets
	**Encryption**	StorCycle Single Key encryption is available for all Target Storage locations. When enabled, all data sent to the target is encrypted. **Note:** Included as a standard feature in Data Center and Enterprise License levels, available for Administrator and Work Group licenses.	Targets
	**Versioning**	Versioning can be assigned to any new NAS Source Storage location and is then enabled for all projects originating from the source. **Note:** The versioning feature enables users to implement targeted backup workflows but does not replace more traditional backup methods. By default, versioning only allows the user to protect file objects.	NAS Sources
	**SMTP**	A Simple Mail Transfer Protocol (SMTP) Server can be configured to enable automatic email alerts for data restores.	Restores and Users
	**Linked Instances**	• An instance of StorCycle can link to one or many other instances of StorCycle on the same network. • From a single StorCycle instance, users can search for files and projects across other linked instances.	StorCycle

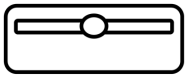
StorCycle Features			
Features		**Description**	**Applies To**
	**Ransomware Protection**	• When using a Spectra BlackPearl NAS target, StorCycle maintains the BlackPearl volume in read-only mode. • StorCycle automatically takes snapshots of a BlackPearl volume after every migrate job.	BlackPearl NAS Target
	**REST API**	Most actions which can be performed in the user interface are available as API commands. Use REST API automation and custom scripting.	StorCycle
	**Throttling**	Control bandwidth allocation for peak and non-peak times for migrations.	Migrate / Store Jobs
	**Filters**	Use Filters to select what type of data to migrate by size, age, type, include / exclude, etc.	Migrate / Store Jobs
	**Tagging**	Apply metadata tags to migrate / store jobs to enhance search capabilities.	Migrate / Store Jobs
	**Retention Policy**	Retention Policies can be assigned to Target Storage locations to expire data after a specified time has passed.	Targets + Migrate / Store Jobs
	**Packing**	Use TAR or ZIP packing with Target locations to maximize the efficiency of migrations.	Targets
	**Transparent Access**	Replace original source files with HTML or Symbolic links to allow users transparent access to data.	Sources and Migrate / Store Jobs and Users

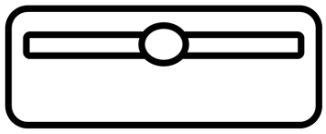
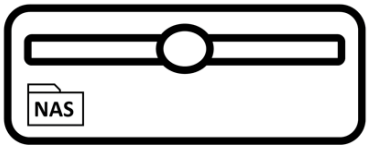
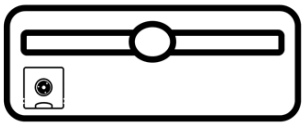
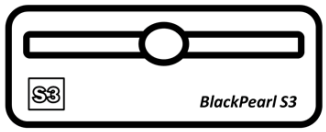
StorCycle Features			
Features		**Description**	**Applies To**
	**Bucket Ingest**	Ingest BlackPearl Target buckets and integrate existing objects into the StorCycle archive database.	BlackPearl Target and Restores
	**Scheduling**	Migrate, Scan, and Restore jobs can be scheduled to run at a future date and time. Migrate and Scan jobs can be configured to run on a recurring schedule.	Migrate / Store Jobs and Scan Jobs and Restore Jobs
	**Database Backup**	Database backups can be manually initiated or set on a recurring schedule.	StorCycle

Migrate / Store Filters **Use filters to ensure that a Migrate / Store job only includes the data you wish to migrate. Filter out files based on object size, age, or type. You can also include only specific file types or exclude specific directories.**		
	**Object Size**	Object Size filters can be applied to Migrate / Store jobs, allowing you to migrate all files which are above a size threshold. • '>1GB' migrates all files which are larger than 1 GB
	**Object Age**	Object Age filters can be applied to Migrate / Store jobs, allowing you to migrate all files which are older than the specified age threshold. • '>2 Years' migrates all files which are older than 2 years
	**Include Type**	Include Type filters migrates the specified file type. • '.PNG' migrates PNG file types
	**Exclude Type**	Exclude Type filters omits the specified file type from being migrated. • '.PNG' migrates any file that is not a PNG file type

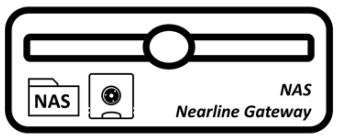
Migrate / Store Filters **Use filters to ensure that a Migrate / Store job only includes the data you wish to migrate. Filter out files based on object size, age, or type. You can also include only specific file types or exclude specific directories.**		
	**Include Directory**	Include Directory allows you to include a specific directory or all directories with the specified name. • '\\production' includes the 'production' folder from the working root directory • 'production' includes every folder named production, regardless of where it exists in directory structure
	**Exclude Directory**	Exclude Directory allows you to exclude a specific directory or all directories with the specified name. • '\\production' excludes the 'production' folder from the working root directory • 'production' excludes every folder named production, regardless of where it exists in directory structure

Windows Environment: Recommended File and System Permissions **In a Windows environment, special attention is required to configure the StorCycle service account, target storage location, and source location permissions.**		
	**StorCycle Server**	A Service Account must be used to run the StorCycle service. • Local Administrator (**Recommended**) or Domain Administrator • Custom Service Account (Not Recommended): 'Full Control - This Folder, Files, and Subfolders'
	**Source Storage**	• If using a Local or Domain Administrator StorCycle Service account, no special configuration is required • If using a Custom Owner service account - Source, Target, and Service Account permissions must match to avoid metadata errors

Windows Environment: Recommended File and System Permissions **In a Windows environment, special attention is required to configure the StorCycle service account, target storage location, and source location permissions.**		
	**BlackPearl NAS or Windows NAS Target**	StorCycle managed shares created specifically for use by StorCycle. • Local Administrators - Full Control - This Folder, Files, and Subfolders • SYSTEM - Full Control - This Folder, Files, and Subfolders • Remove Domain Administrator if using Local Administrator (and any other group)
	**S3 / Cloud Target**	No special configuration required. • S3 / Cloud Targets include: AWS, AWS Glacier, MS Azure Archive, Standard S3 targets

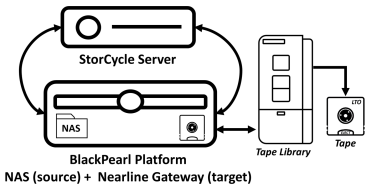
Spectra's BlackPearl Platform		
	BlackPearl Platform Spectra's BlackPearl platform can be configured in multiple combinations to support NAS, S3, and a Nearline gateway. The following workflow configurations use the base BlackPearl images with a NAS, Nearline, and S3 icon, to indicate how the system is configured.	
		BlackPearl NAS • Secondary NAS Storage • Support for Ransomware protection
		BlackPearl Nearline Gateway • Gateway to Tape archive • Object Storage Disk
		BlackPearl S3 • BlackPearl with S3 support

Spectra's BlackPearl Platform



BlackPearl Nearline Gateway + BlackPearl NAS

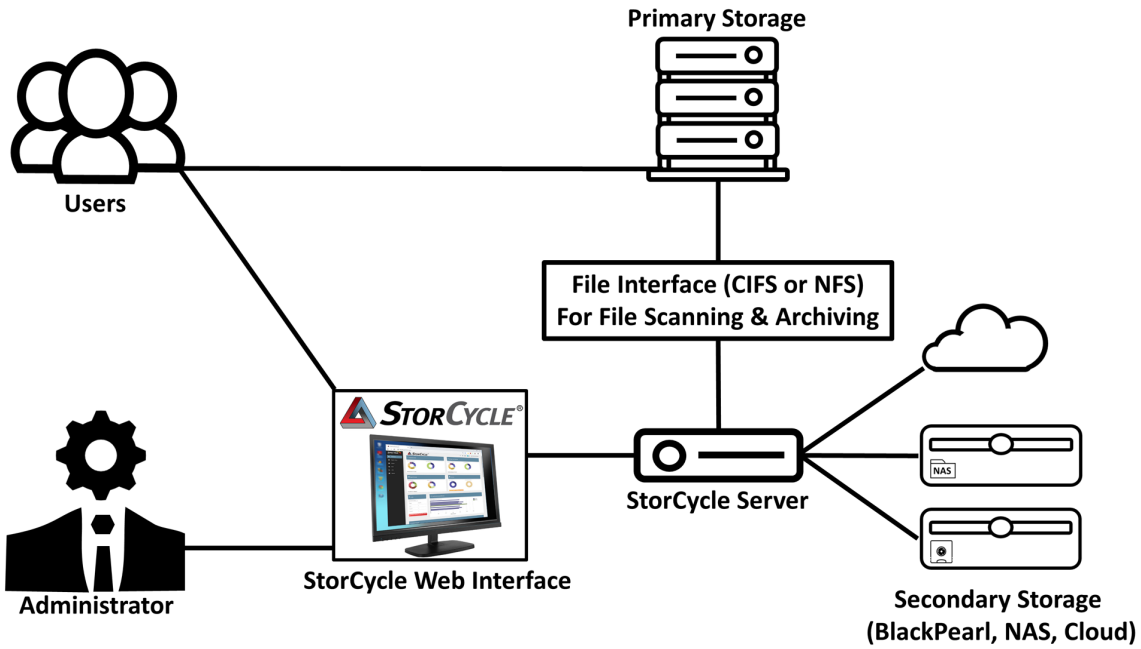
- A BlackPearl platform can be configured to support both NAS and a Nearline gateway



StorCycle + BlackPearl Platform + Tape Library

- A single BlackPearl can be configured for both NAS and Nearline Gateway
- BlackPearl NAS can serve as the Source Location
- Nearline Gateway can serve as Target Location
- Nearline Gateway moves data to tape library

Basic Workflow



A standard StorCycle workflow has the StorCycle solution installed on a virtual machine or dedicated server. Primary storage will mount to the server/VM via CIFS or NFS. Target NAS storage is also mounted on the StorCycle server. S3 Sources/Targets and BlackPearl targets will connect using S3 credentials. Users and Administrators interact with StorCycle through the StorCycle web interface, the API, or by using HTML or Symbolic Links for transparent access to data.

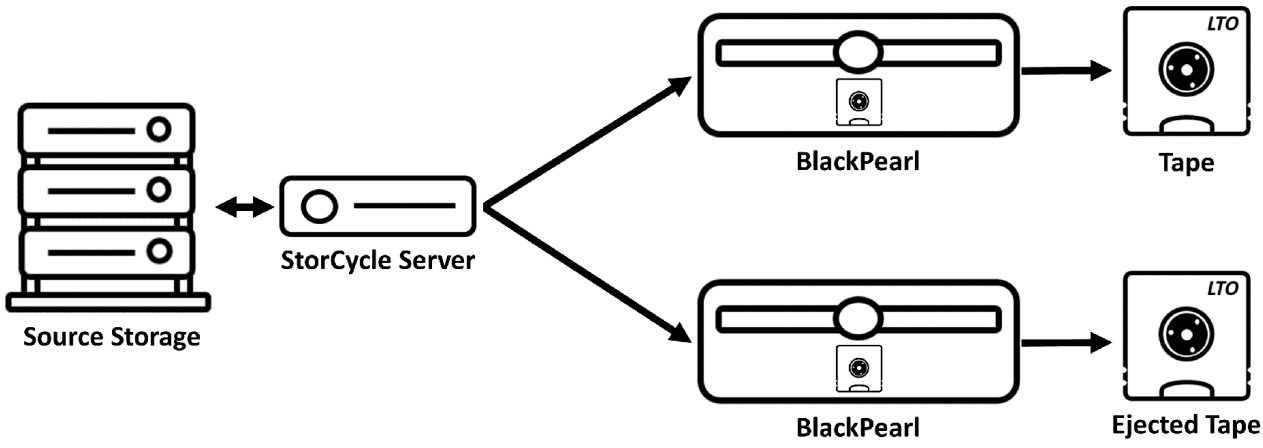
StorCycle can be configured to scan Source Storage locations on a schedule or when triggered. Storage Managers and Administrators can then configure Migrate / Storage jobs to move all files or just a subset of the files based on age, size, and type filters. After files are migrated, the original source files can remain on source storage, be removed, or replaced with HTML or Symbolic links to provide transparent link access to end users.

Both Files and HTML links can be restored from the user interface by restoring specific Migrate / Store jobs, portions of Migrate / Store jobs, or individual files. Restores can move files to the original Source Location or to a new location. Using StorCycle's robust search feature, users can search for files by project name, file name, or tag.

Reference Workflows

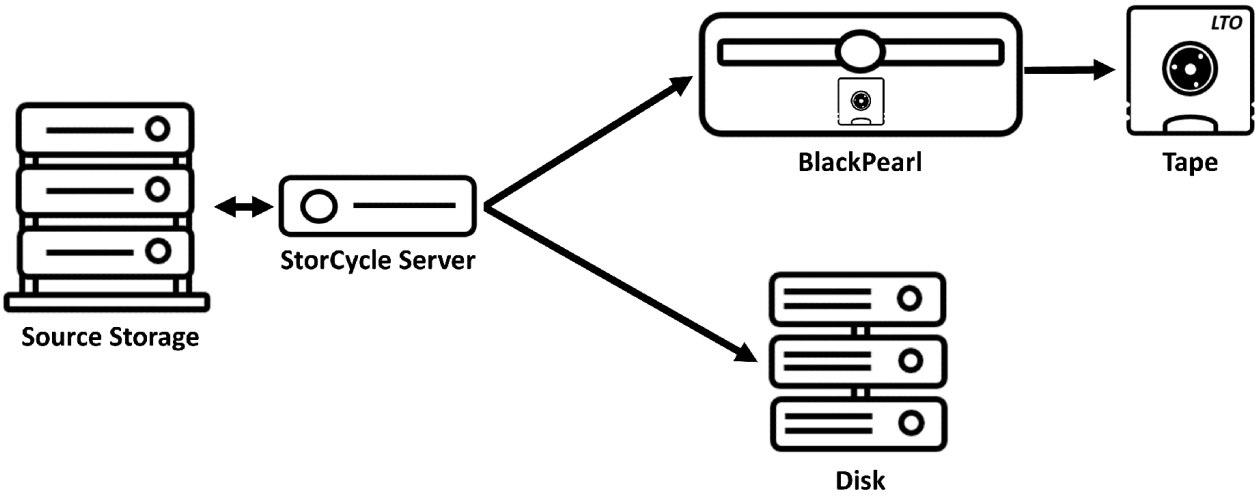
Tape + Tape (Ejected)

A single StorCycle project or job can migrate files to multiple storage targets. Using a single BlackPearl system, StorCycle can write to two BlackPearl buckets with one bucket writing a copy to tape, and the other bucket writing and ejecting the tape. A similar workflow can also be accomplished with a single bucket in BlackPearl, using BlackPearl data policies to write two copies with one copy then ejected. Spectra Logic tape libraries support both LTO and TS11xx technologies.



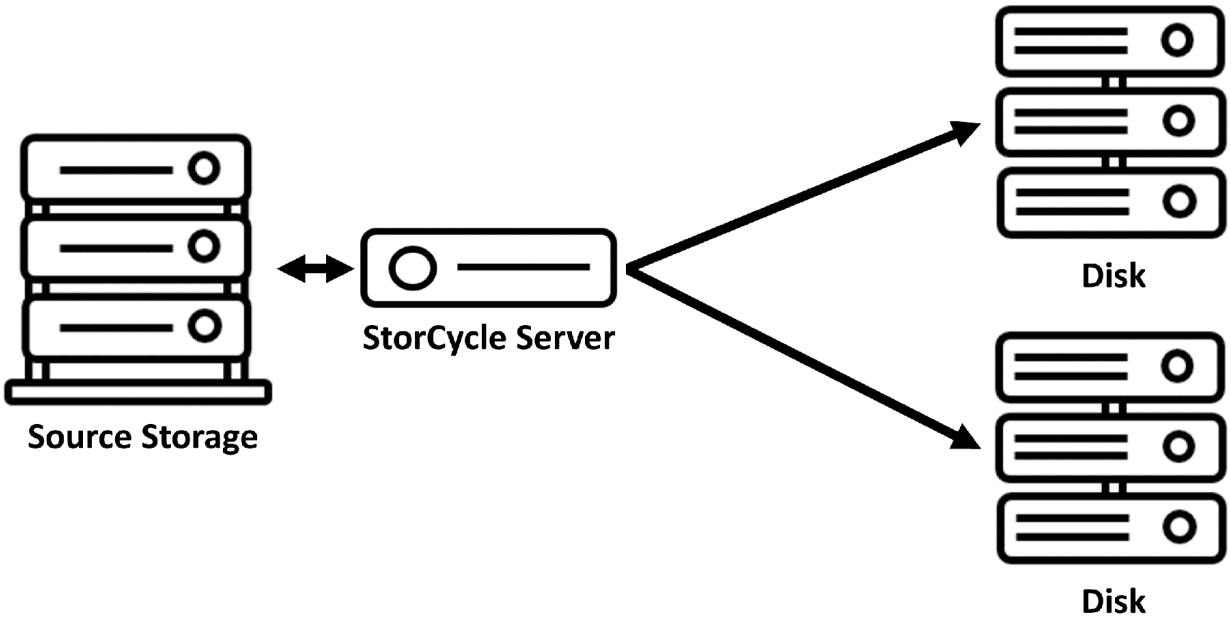
Tape + Disk

Different target types can be used in a single project or job to write a copy of data to a tape library and a second copy to secondary disk.



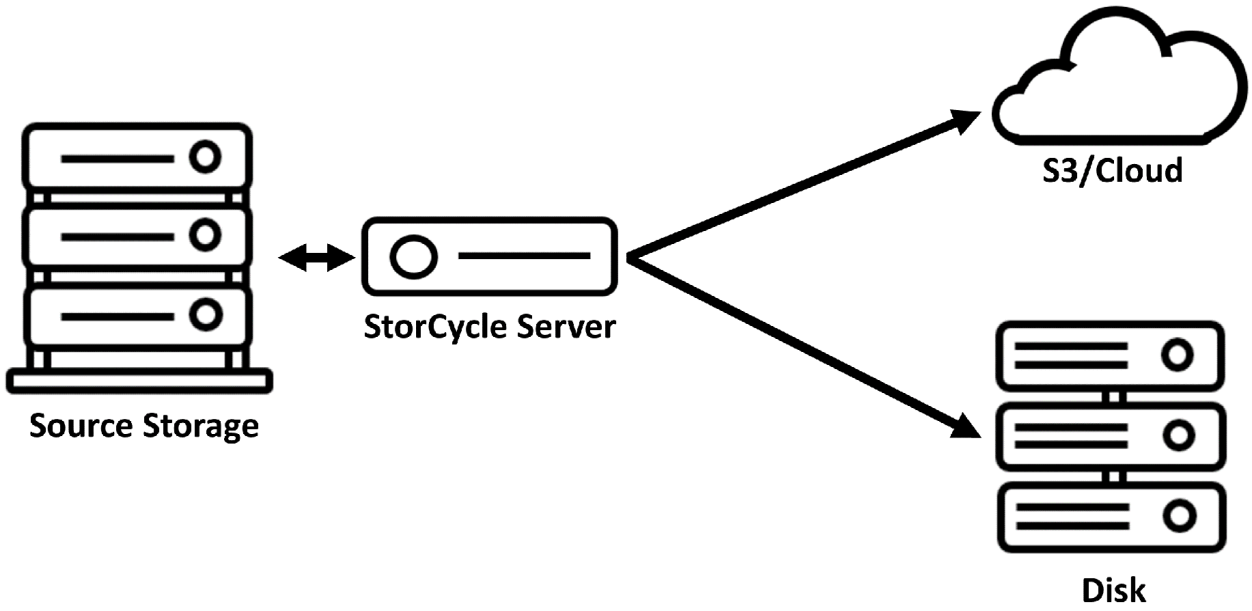
Disk + Disk

Multiple NAS Target Locations can be used in a single project or job.



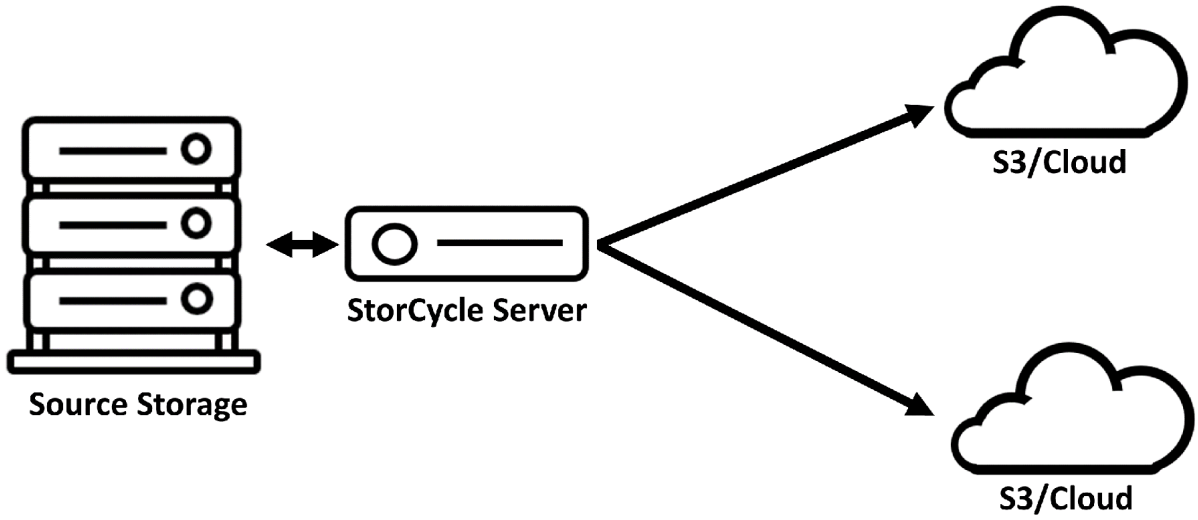
Cloud + Disk

StorCycle's S3 Target Locations can be used for standard cloud storage, such as AWS, and also be used for standard S3 appliances. S3 and disk targets can be mixed on a single project or job.



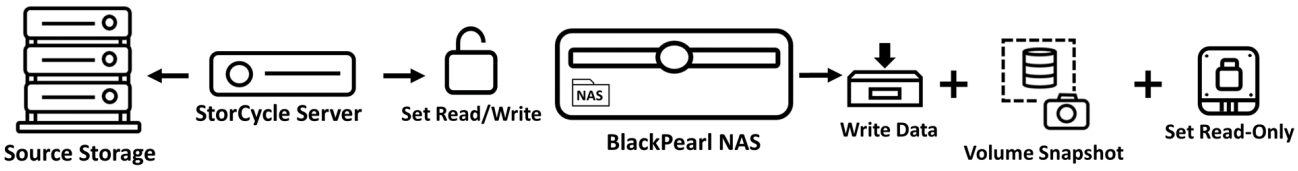
Cloud + Cloud

Multiple S3 Target Locations can be used in a single project or job.



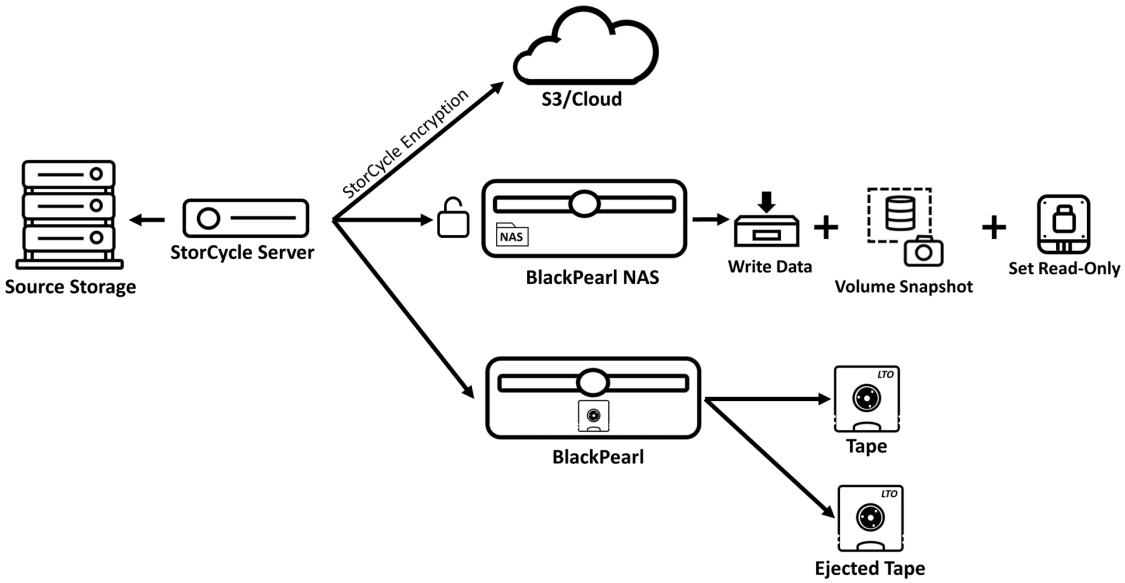
Ransomware Snapshot Protection

When using a BlackPearl NAS target, StorCycle can be configured to automatically maintain the BlackPearl volume in a read-only state. StorCycle also automatically takes volume snapshots at the end of each Migrate / Store job and File / Delete job (retention policy, version delete, etc.)



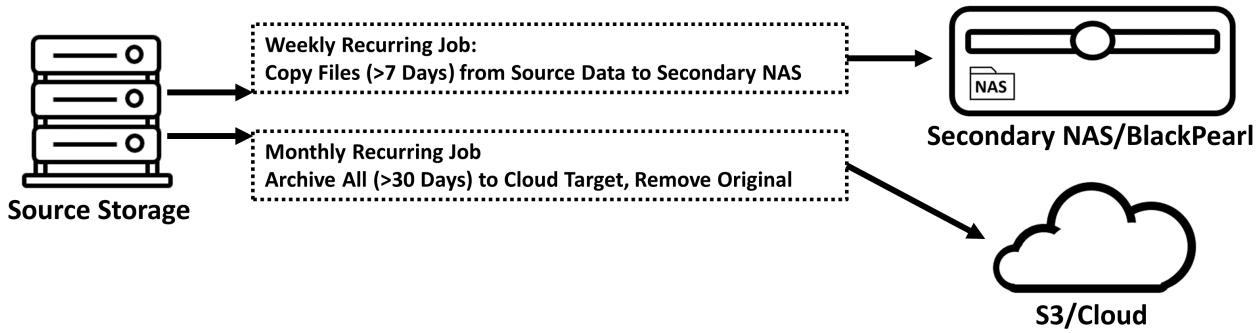
Cloud (encrypted) + BlackPearl NAS Ransomware + Tape (2 copies, 1 ejected)

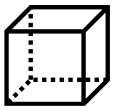
StorCycle supports up to 3 Target Locations in a single Project / Job. This example uses StorCycle encryption for the cloud target, a ransomware protected copy on a BlackPearl NAS, and a single copy sent to a BlackPearl bucket which uses a dual-copy data policy (2 copies on tape, one copy ejected).



Versioning Workflow

StorCycle Versioning allows for many different types of workflows. Below is an example of StorCycle Versioning, moving the same source data to two different filters and retention policies. The weekly project is moving all data that is older than 7-days to a secondary NAS target with a 30-day retention policy. The monthly project is moving all data older than 30-days to a cloud target for long-term archive.



Data Protection Strategies		
	**Encryption**	Encryption can be enabled for any Target Location. When enabled, every file or object sent to the target will be encrypted using StorCycle controlled single key encryption.
	**Domain Groups**	A single domain group can be applied to a source storage location. The location is then restricted to Domain Users who are members of the group and Administrators.
	**Versioning**	Versioning is assigned to Source Locations. Once enabled, StorCycle makes a version of the source file with each migrate job. Versioning can be configured to: • Version file on every Migrate / Store job. • Version only files which have changed since the last job. • Optionally maintain a certain number of versions on Target Locations.
	**Ransomware Protection**	Ransomware Protection is delivered by using a BlackPearl NAS Target location. When enabled, StorCycle maintains read-only access on the BlackPearl NAS volume and triggers volume snapshots at the end of every job.
	**Retention Policy**	Retention Policies can be assigned to Target Locations. For example, with a retention policy of '30' days, StorCycle deletes archived data from the targets 30 days after the completion of the archive.
	**Transparent Access**	Transparent Access for end users can be provided with Symbolic Links or HTML Links. Symbolic Links are supported on NAS targets only and allow users to access the Symbolic Link from the Source location without a data restoration. HTML Links replace original source files with a HTML file that end users can use to access the StorCycle user interface for data restoration or to send a restore request to a StorCycle Administrator.

Performance Strategies		
	**Throttling**	Apply job throttling to Migrate / Store jobs to reduce performance during peak work-hours. You can set peak hour schedule and bandwidth caps.

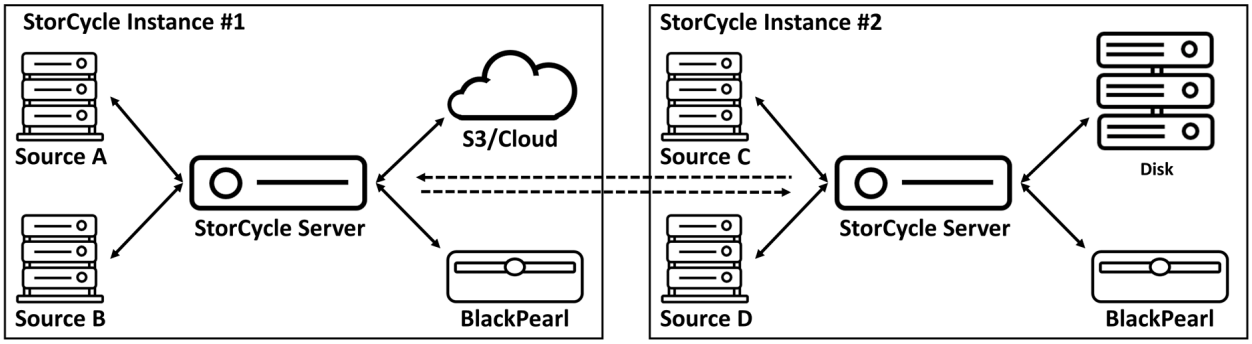
Performance Strategies		
	**Filters**	Use filters on Migrate / Store jobs to only migrate specific sized files, files which meet a particular age criteria, specific file types, and other exclusion types. For example, if a single source has many files which are both very large and very small, a job could be configured to move the large files separately and then move the smaller files with packing enabled on a BlackPearl.
	**Packing**	On targets, Packing can be enabled, which will split a Migrate / Store job into several ZIP or TAR packages, minimizing the total objects transferred and improving archive, search, and restore performance.
	**Scheduling**	Scheduling is used to configure a job to run at a future time. This can be used to run a large scan job during off hours. Scheduling is also used to create recurring scan or Migrate / Store jobs. For example, a scan job could be scheduled to run on the weekend, and a recurring Migrate / Store job could use the scan data to move data every Monday.
	**Professional Services Tuning**	Please work with Spectra Logic Professional Services if changes to StorCycle's configuration for performance is required.

Linked Instances

StorCycle can connect to other StorCycle instances on the same network and allow users to search the connected databases for archived files.

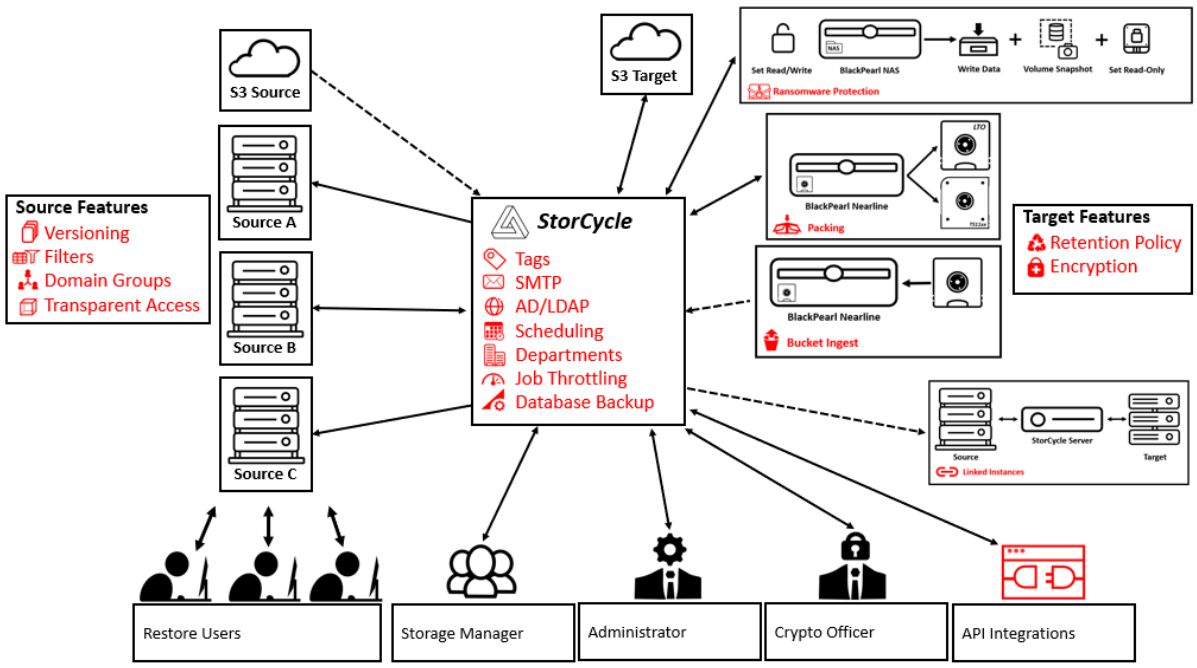
In the example below, StorCycle Instance #1 can make a connection to Instance #2 to allow users to search for any file which was archived by either system. When ready to restore data, users will be guided to the user interface of the instance where their data is located. The sources and targets remain independent between the two instances: Source A and Source B can only archive data to S3 / Cloud and BlackPearl NAS. StorCycle Instance #1 can also only be restored to either Source A or Source B.

When StorCycle Instance #1 connects to Instance #2, it is a one-way connection and Instance #2 will not be able to search the archived contents in Instance #1. However, Instance #2 can configure its own connection in order to be able to search for archived files of Instance #1.



StorCycle Master Diagram

The diagram below displays a fully featured workflow utilizing many of the StorCycle features and workflows available. Features in RED are optional.



Restore Users	Storage Managers	Administrator	Crypto Officer	API Integrations
• Requires AD/LDAP configuration. • Can access HTML links. • Can restore user interface. • Access restricted with domain groups.	• Can configure jobs. • Cannot configure storage locations or settings. • Access restricted with domain groups.	• Default Administrator. • Super user with unrestricted access.	• Full Administrator permission. • Can configure and set encryption.	• Available OpenAPI for integrations.

LICENSING

The Spectra StorCycle solution is available with two licensing models, a permanent license and an annual subscription. These models give greater flexibility for organizations to choose whether they want to use the StorCycle solution as a capital or operational expenditure.

StorCycle License Model

The Spectra StorCycle solution supports four different types of licenses - Administrator, Workgroup, Data Center, and Enterprise. Each license supports a different quantity of named users, which use any of the licenses to connect to an unlimited number of primary storage sources and Spectra storage targets. Each StorCycle license provides some free licensing for migrating to the cloud and non-Spectra NAS.

License	Users	Free Cloud Storage Access	Free Non-Spectra NAS Storage Access
Administrator	3	25 TiB	1 TiB
Workgroup	25	50 TiB	1 TiB
Data Center	100	100 TiB	1 TiB
Enterprise	unlimited	unlimited	1 TiB

Additional Non-Spectra storage targets (Cloud and NAS storage products not provided by Spectra Logic) can be added for an additional price, based on the number of terabytes (TiB) of storage being used.

Notes:
- Restore only Active Directory® / LDAP users (see Configure Active Directory / LDAP on page 137) count against the licensed user limit.
- The default "Administrator" account is included against the limit, so for example, the Administrator license would allow 2 more users.

USING ANTI-VIRUS SOFTWARE WITH THE STORCYCLE SOLUTION

The use of antivirus or scanner software including Cloudstrike™, AVAST®, Norton™, Sophos™, and other antivirus software greatly impacts performance and is not supported for use with the StorCycle solution. The performance impact of such software is not a valid reason for support escalation with Spectra Logic Technical Support. A regular scheduled scan of the StorCycle server is recommended during off hours. Real time scanning is not supported.

Chapter 2 - Install the StorCycle Solution on a Windows Server

This section describes how to do the initial installation of the Spectra StorCycle Solution on a Windows server. For instructions to upgrade to a newer version of the Spectra StorCycle Solution see Upgrade the StorCycle Solution on page 244.

The StorCycle solution is intended to migrate / store or copy inactive files. It is not intended to backup or manage active files in primary storage.

IMPORTANT

The StorCycle solution runs on Windows servers and supports CIFS/SMB networked storage or runs on Linux servers and supports NFS-protocol storage or CIFS/SMB networked storage.

If you are installing StorCycle on a Linux server, see Install the StorCycle Solution on a Linux Server on page 62.

VERIFY STORCYCLE REQUIREMENTS

Ensure that the server you will use for StorCycle meets the following minimum requirements:

Notes:
- Additional RAM and CPU cores will improve file transfer speeds in most cases.
- Customers are responsible for maintaining patches and upgrades on the operating system where StorCycle is installed.

- 64 GB RAM
- Four 64-bit CPU cores running at a minimum of 2.6 GHz
- 1 TB hard drive space for the StorCycle solution
- 4GiB database drive space per 10 million files scanned/migrated.
- 10 GigE network or better
- Windows Server® 2019
- A network which supports reverse DNS lookups. If the network does not support reverse DNS lookups, then the IPv4 address of the storage location is used in HTML links created during a Migrate / Store job. See Migrate / Store Wizard—Set Targets on page 174 for more information.
- The StorCycle solution uses whatever domain is configured on the server, including multiple / trusted domains, to access DNS (Domain Name System) to resolve UNC (Universal Naming Convention) paths over the domain and uses Active Directory / LDAP to verify restore users are valid on the domain.
- If storage locations are configured to group files into TAR or ZIP 'packs', the data to be packed is temporarily written to the server disk storage before it is transferred.
  - When using packing, the StorCycle solution requires enough disk space on the drive for ten times the size of a pack (10 * 10 GiB), or the largest file to be migrated / stored in a pack, whichever is larger.
  - For maximum performance, Spectra Logic recommends that flash / SSD storage be used for the StorCycle server disk storage when creating TAR or ZIP packs.
  - Packing may use up to 500 GiB and the MongoDB will require (minimum) 4 GiB per 10 Million Files (assuming that no files being packed are larger than 10 GiB).
- Due to Windows limitations, the file system must meet the following requirements:
  - Maximum file directory path length determined by the Windows Server version.
  - Maximum directory depth determined by the Windows Server version.
- The user interface supports Google Chrome version 75 or later and requires a minimum screen resolution of 1024 pixels.

CONFIGURE THE USER ACCOUNT

The StorCycle installation includes two services, the StorCycle service and the MongoDB® service. By default, these services are run by the Local System User. However, the Local System User often does not have access to all storage locations used by the StorCycle solution, permissions to read from and write to the storage locations, and permissions to take ownership of files. If you want to use the Local System User to run the services, continue with Download and Install the StorCycle Software on page 57.

If you want to configure a different user to run the StorCycle service, use the table below to select the privileges to configure.

Note: Consult an IT administrator to configure the StorCycle service user.

Note: If you plan to create NAS storage targets, see Source Storage Location Best Practices - NAS Storage on page 82before continuing.

Role	Privileges	Configuration Instructions
Domain Administrator - **Recommended**	• Able to migrate / restore any files and folders on a computer in the domain, with or without a two-way trust relationship. • The StorCycle user is added to the Domain Administrator Group for the entire Domain.	Configure a Domain Administrator on the next page
Local Administrator - **Recommended**	• Able to migrate / restore files and folders on the local computer to which the local group applies. • StorCycle user added to 'Local Administrator' group on the StorCycle Server and ALL Source and Target shares.	Configure a Local Group Administrator on the next page
Custom Owner of Files and Folders - **Not Recommended**	• Custom attributes to give a StorCycle user special privileges to perform actions such as taking control of files, or creating symbolic links. • A user or group with 'Full Control' and special attributes is created and added to all Source and Target shares.	Configure a Custom Owner of Files and Folders on page 48

Configure a Domain Administrator

Domain Administrator users have unrestricted access to all files and folders on the domain. With this configuration, an IT Administrator adds the StorCycle user to the Domain Administrator group.

1. Create a user account for running the StorCycle service.

Notes:
- If you want to use the same user as your Spectra NAS equipment, use all lower case for the username.
- Spectra Logic recommends that you select the **User cannot change password** and **Password never expires** check boxes when creating the new user.

2. Add the new user account as a member of the Domain Administrators group.

Note: The user must be an Administrator and not a Backup Operator. Windows does not give Backup Operators permissions to write files and cannot be used to create HTML links and symbolic links on sources, or write files to most targets.

3. Spectra Logic recommends mounting Isilon CIFS shares for the user running the StorCycle solution using the "map network drive" wizard or the "net use" command.
4. Continue with Download and Install the StorCycle Software on page 57.

Configure a Local Group Administrator

Local Administrator group users have unrestricted access to files and folders on the StorCycle server, NAS sources, and NAS targets. An IT Administrator must manually add the StorCycle user to each Local Administrator group on every required server.

1. Create a User Account for running the StorCycle Service.

Notes:
- If you want to use the same user as your Spectra NAS equipment, use all lower case for the username.
- Spectra Logic recommends that you select the **User cannot change password** and **Password never expires** check boxes when creating the new user.

2. Make the new user account a local Administrator on the StorCycle server, all source locations, and all target storage locations.

Note: The user must be an Administrator and not a Backup Operator. Windows does not give Backup Operators permissions to write files and cannot be used to create HTML links and symbolic links on sources, or write files to most targets.

3. If migrate / store projects will replace files with symbolic links for transparent access, ensure the new user can create symbolic links.
   a. Use the keyboard shortcut Windows logo key+R to open the Run window.

b. In the Open: field enter `secpol.msc` and click **OK**. The Local Security Policy window displays.

c. Select **Local Policies > User Rights Assignment**, and then double-click **Create symbolic links**. The Create symbolic links Properties screen displays.

d. Add the Service User account name created in Step 1 on page 47.

4. Spectra Logic recommends mounting Isilon CIFS shares for the user running the StorCycle solution using the "map network drive" wizard or the "net use" command.
5. Continue with Download and Install the StorCycle Software on page 57.

Configure a Custom Owner of Files and Folders

If Domain and Local Administrators cannot be used, custom security policy attributes must be added to the account or custom group to access each source and target share.

Create a new user account for running the StorCycle service

1. Use the keyboard shortcut Windows logo key+R to open the Run window.
2. In the **Open:** field enter `lusrmgr.msc` and click **OK**. The Local Users and Groups window displays.
3. Select the **Users** folder and select **Action > New User**. The New User dialog box displays.

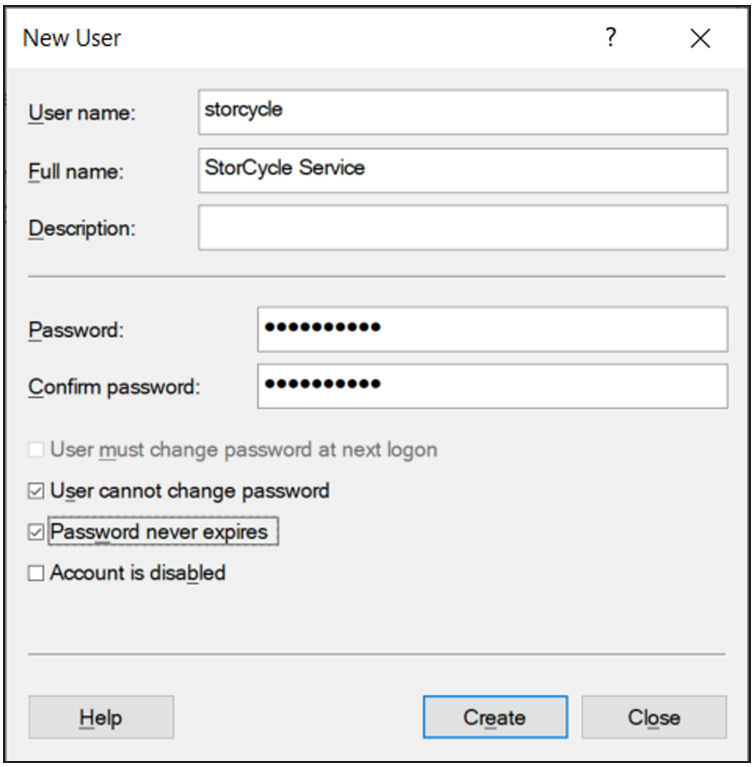


Figure 2 The New User dialog box.

4. Create a new user account that will be used for the StorCycle service.

Notes:
- If you want to use the same user as your Spectra NAS equipment, use all lower case for the username.
- Spectra Logic recommends that you select the **User cannot change password** and **Password never expires** check boxes when creating the new user.

   a. Provide values for **User name** (for example, storcycle), **Full name**, and **Password**. Record this information.

   b. Clear the **User must change password at next login** check box.

   c. Select the **User cannot change password** and **Password never expires** check boxes.

   d. Click **Create** and click **Close**.

Give the new user account the privileges necessary for the StorCycle solution

If network access is restricted by group, add the Service User Account to Groups with access to every share that you want to access with the StorCycle solution.

Note: If the user under which the StorCycle service is running has read-only permissions to a directory on a source storage location, then StorCycle will be unable to place files into the directory with the same name created on a NAS target storage location because the directory will have the same read-only permissions.

1. Select the **Groups** folder. The list of all available groups displays.
2. Select a Group that you want to add the Service User Account to and select **Action > Add to Group**. The *Group* Properties dialog box displays.
3. Click **Add**. The Select Users, Computers, Service Accounts, or Groups dialog box displays.

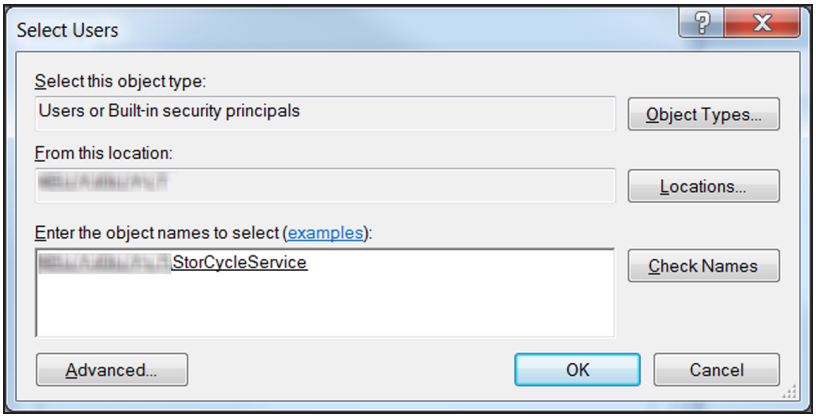


Figure 3 The Select Users, Computers, Service Accounts, or Groups dialog box.

4. In the **From this location** field, select the name of the server. The dialog box changes to Select User.
5. In the **Enter the object names to select** field, enter the Service User Account name created in Create a new user account for running the StorCycle service on page 48 and click **Check Names**.
6. Click **OK** to add the Service User Account to the Group.
7. Repeat to as needed to add the Service User Account to additional groups.

Give the new user account full control of the program data directory

1. Open File Explorer.
2. Browse the system or network drive for the **ProgramData** file.

Note: ProgramData is a hidden folder, you may need to change File Explorer options to see it.

3. Right click the Spectra Logic Corporation directory and select **Properties**. The Spectra StorCycle Properties screen displays.

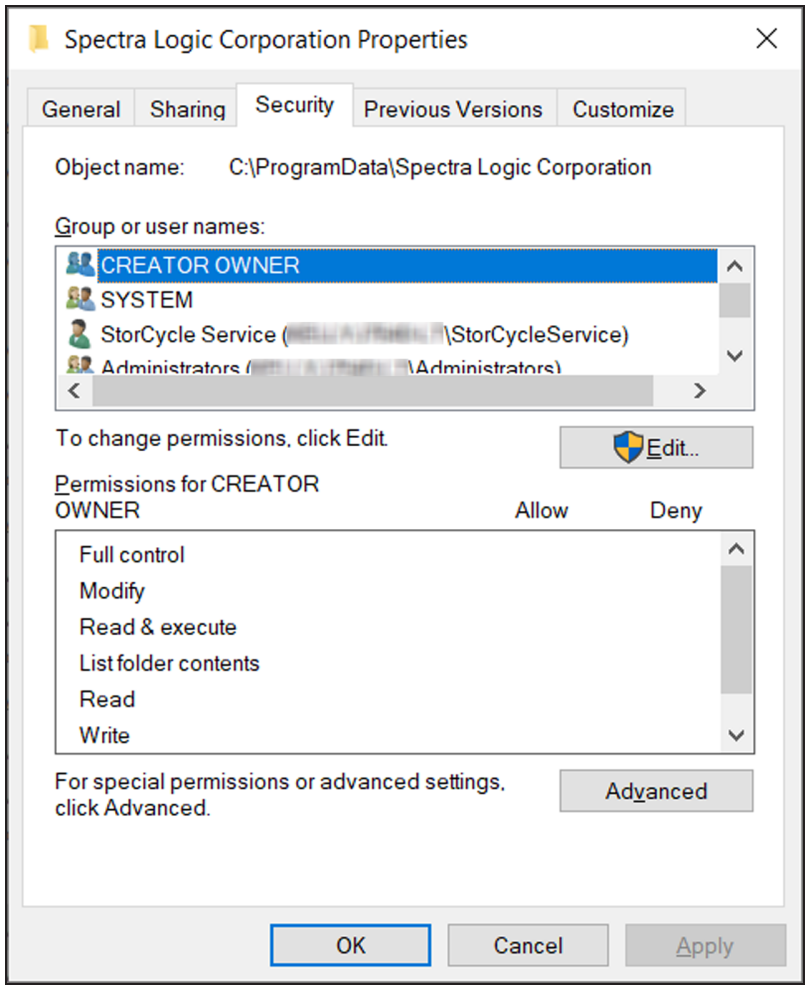


Figure 4 The Spectra Logic Corporation Properties dialog box.

4. Select the **Security** tab and click **Edit**, then click **Add**. The Select Users, Computers, Service Accounts, or Groups dialog box displays.

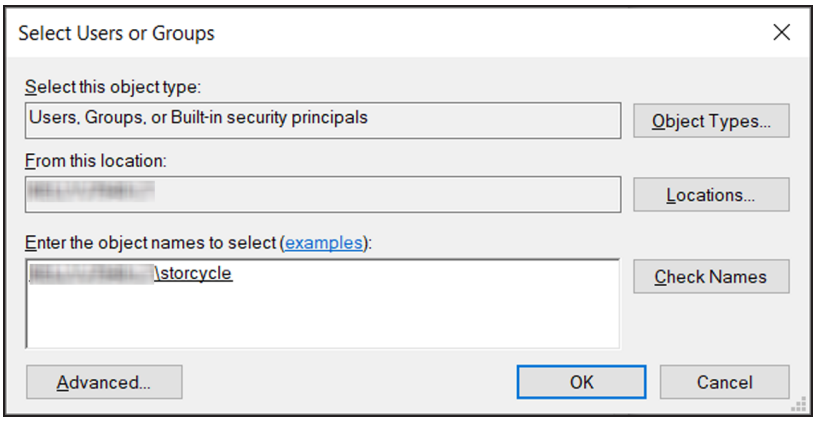


Figure 5 The Select Users, Computers, Service Accounts, or Groups dialog box.

5. Click **Locations**, select local computer, and then click **OK**. The dialog box changes to Select Users or Groups.
6. In the **Enter the object names to select** field, enter the Service User account name created in Configure a Custom Owner of Files and Folders on page 48 and click **Check Names**, then click **OK**.
7. Select the newly created Service User account in the **Group or user names** field. In the **Permissions for** pane, in the **Allow** column, select **Full Control**, and click **OK**.
8. Click **OK** again.

Configure the new user account to take ownership of files and other objects

1. Use the keyboard shortcut Windows logo key+R to open the Run window.
2. In the **Open:** field enter `secpol.msc` and click **OK**. The Local Security Policy window displays.
3. Select the Local Policies folder in the left pane, and double-click **User Rights Assignment** in the right pane.
4. Double-click the policy **Take ownership of files and other objects**. The "Take ownership of files and other object Properties" dialog box displays.
5. Click **Add User or Group...**. The Select Users, Computers, Service Accounts, or Groups dialog box displays. See Figure 3 on page 49.
6. Click **Object Types**. The Object Types dialogue box displays.
7. Select all of the Object types listed and click **OK**.

8. Click **Locations** and select the name of the server and click **OK**. The dialog box changes to Select Users or Groups.
9. In the **Enter the object names to select** field, enter the Service User account name created in Configure a Custom Owner of Files and Folders on page 48 and click **Check Names** and then click **OK**.
10. Click **OK** again.

Configure network drive access for the new user account

The user running the StorCycle service must be able to access and have permission to read and write on all of the storage locations in the StorCycle environment.

Notes:
- If the user under which the StorCycle service is running has read-only permissions to a directory on a NAS source storage location, then StorCycle will be unable to place files into the directory with the same name created on the target storage location because the directory will have the same read-only permissions.
- Spectra Logic recommends mounting Isilon CIFS shares for the user running the StorCycle solution using the "map network drive" wizard or the "net use" command.

1. Sign in to Windows using the new user account created in Configure a Custom Owner of Files and Folders on page 48.
2. Open File Explorer.
3. Select **This PC** on the left.
4. Click **Map Network Drive**. The Map Network Drive dialog box displays.
5. Select a drive letter and enter a folder path for a Storage Location you want to use in the StorCycle solution.
6. Select **Reconnect at sign-in** and **Connect using different credentials**.
7. Click **Finish**.
8. Enter the credentials for the user account you want to use to connect to the NAS storage location. Select **Remember my credentials** and then click **OK**.
9. Repeat through for additional NAS storage locations.

Configure NAS share access for the new user account

If the user running the StorCycle service is used to Migrate / Store data to a NAS storage location, configure the permissions as described below.

1. Sign in to Windows using the new user account created in Configure a Custom Owner of Files and Folders on page 48.
2. Open File Explorer.

3. Navigate to the NAS share, or a folder in the NAS share.
4. **Right-click** the share, then select **Properties**.
5. Select the **Security** tab, then click **Advanced**. The Advanced Security Settings screen displays.

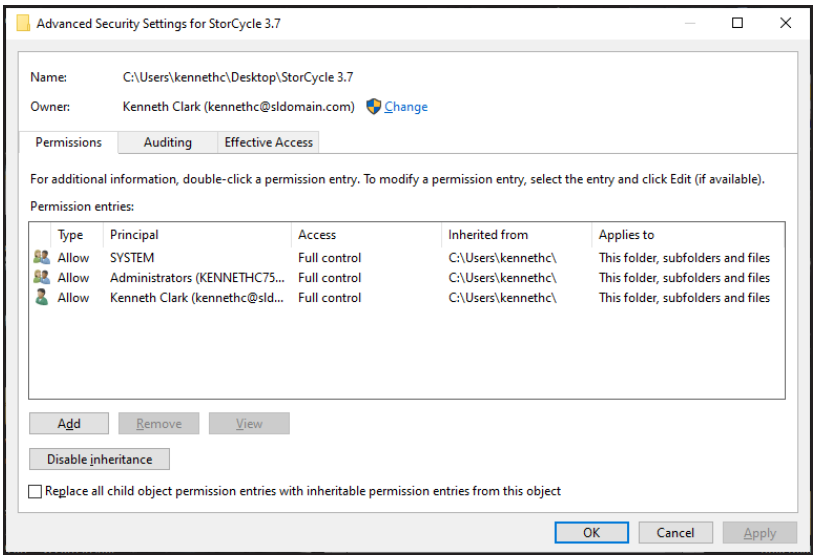


Figure 6 The Advanced Permission Settings.

6. Click **Add**. The Permission Entry screen displays.

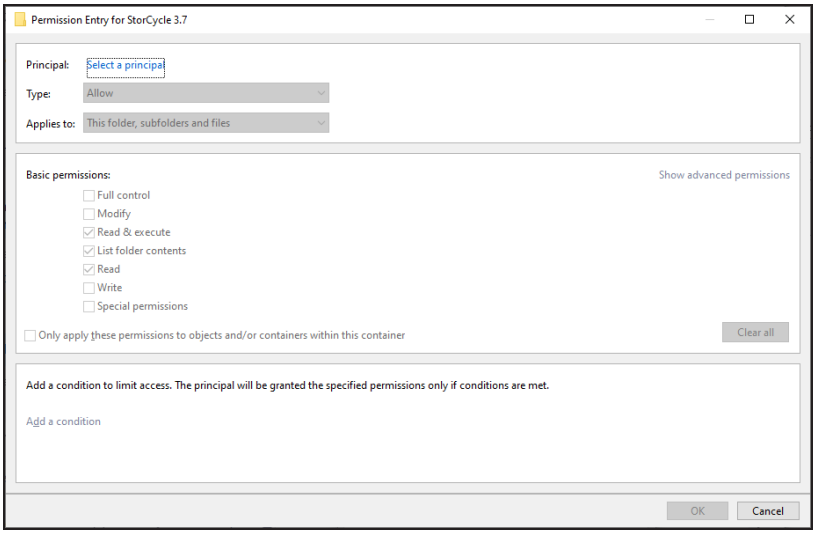


Figure 7 The Permissions Entry screen.

7. If necessary, select a **Principal** user.
8. Using the **Applies To** drop-down menu, select **This folder, files and subfolders**.
9. Under **Basic Permissions**, select **Full Control**.

10. Click **OK** to close the Permissions Entry screen, then click **OK** to close the Advanced Permission Setting screen.
11. Click **OK** to close the Folder Properties screen.
12. Repeat through for additional NAS storage locations.

Give a new user the ability to create symbolic links

If migrate / store projects will replace files with symbolic links for transparent access, ensure the new user can create symbolic links.

1. Use the keyboard shortcut Windows logo key+R to open the Run window.
2. In the Open: field enter `secpol.msc` and click **OK**. The Local Security Policy window displays.
3. Select **Local Policies > User Rights Assignment**, and then double-click **Create symbolic links**. The Create symbolic links Properties screen displays.
4. Add the Service User account name.

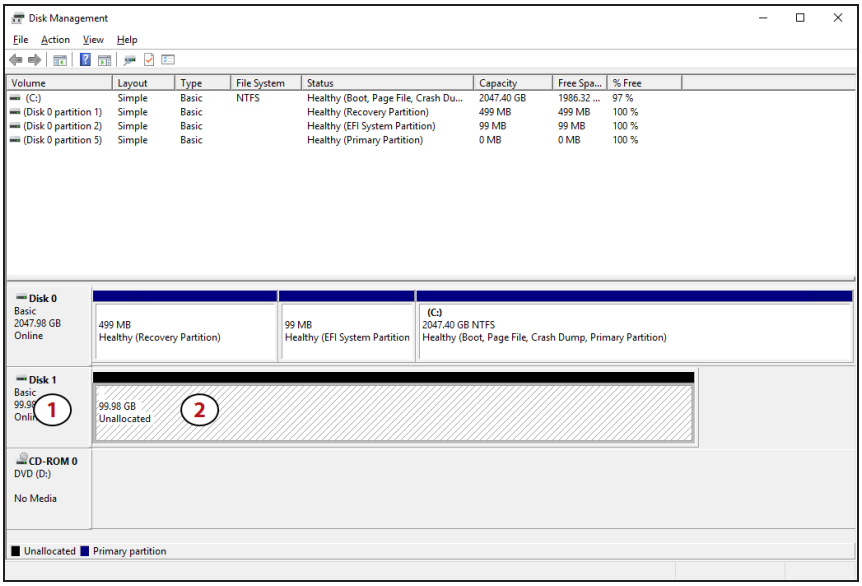
CONFIGURE VOLUME SNAPSHOTS FOR THE STORCYCLE DATABASE - WINDOWS

Before you can install the StorCycle solution, you must configure your system to create volume snapshots for the StorCycle database.

Use the instructions in this section to configure volume snapshots in a Windows environment.

Note: The below commands require Administrator privileges.

1. Create a new volume and assign it as drive letter.
   a. On your keyboard, press with **Windows + R** keys. The Run window displays.
   b. Enter `diskmgmt.msc`. The Disk Management window displays.



   c. Locate the row of the disk on which you want to create a new volume.
   d. If necessary, initialize the disk by right-clicking on the disk number (**1**) and selecting **Initialize Disk**.
   e. To create the volume, right-click the unallocated volume (**2**) and select **New Simple Volume**. The New Simple Volume Wizard displays.
   f. Click **Next** to start the wizard.
   g. On the Specify Volume Size screen, if desired, change the pre-entered value for **Simple volume size in MB**, and click **Next**.
   h. On the Assign Drive Letter or Path screen, if necessary, select **Assign the following drive letter:**, then use the drop-down menu to select a drive letter.
   i. Click **Next**.

j. On the Format Partition screen, select **Format this volume with the following settings**.

k. Configure the following settings for the volume:

- Using the **File system** drop-down menu, select **NTFS**.
- Select your desired **Allocation unit size**.
- Enter the desired **Volume Label**.
- Select **Perform a quick format**.
- Make sure **Enable file and folder compression** is cleared.

IMPORTANT **Do not** use file and folder compression when creating a volume to store database snapshots.

l. Click **Next**. On the Summary screen, verify all information is correct, then click **Finish**.

2. Open a command prompt. On your keyboard press **Windows + R**. The Run window displays.
3. In the entry field, type `cmd` and click **OK**.
4. Enter the following command to created a test snapshot.

   ```
   vssadmin create shadow /for=<drive_letter>:
   ```

   where <drive_letter> is the letter assigned to the drive in Step h on page 55.
5. Verify the test snapshot was created successfully:

   ```
   vssadmin list shadows
   ```
6. Delete the test snapshot:

   ```
   vssadmin delete shadows /for=<drive_letter>:
   ```

   where <drive_letter> is the letter assigned to the drive in Step h on page 55.
7. During the StorCycle solution installation, specify the new volume path for the database.

DOWNLOAD AND INSTALL THE STORCYCLE SOFTWARE

Use the following instructions to download and install the software.

1. Sign in to the server where you want the program to run as a user that is a member of the "Administrators" Local Group.
2. Download the Spectra StorCycle solution installer.
3. Run the installer, `ssc.revision.msi`, where *revision* is the revision number for the software.
4. Follow the on-screen instructions to install the software until you reach the Service Account screen.

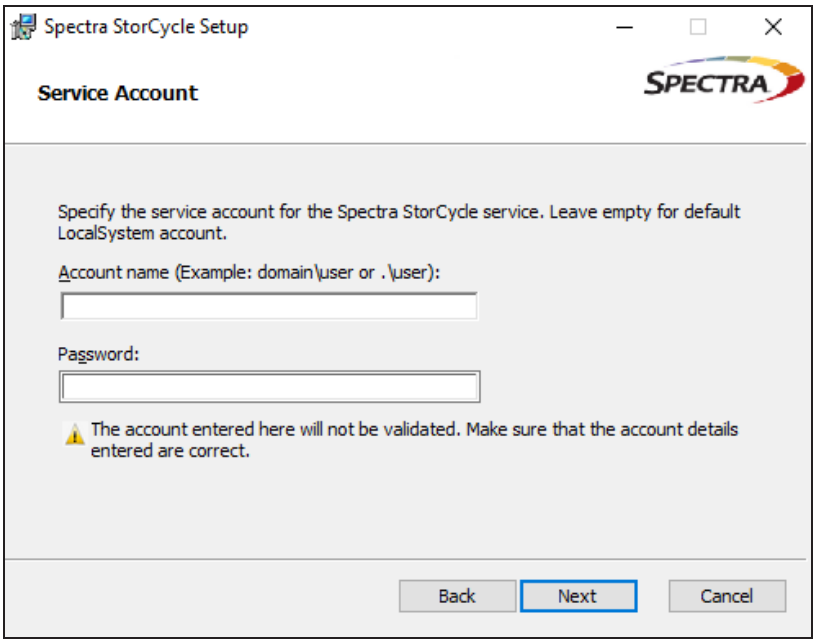


Figure 8 The Service Account screen of the StorCycle install wizard.

5. On the Service Account screen, do one of the following:
   - Leave the **Account name** and **Password** fields empty if you want the Spectra StorCycle service to run under the Local System user.

     -OR-

   - Enter the **Account name** and **Password** you created in Configure the User Account on page 46.
6. Click **Next** and continue to follow the installation steps.
7. When the product installation completes, click **Finish** to close the install wizard.

ENABLE LONG PATHS

A Windows host system running the StorCycle application must be configured to use long file paths. Enabling long file paths increases the number of characters allowed in a file and directory path name from 260 characters to 32,767 characters.

Enabling long paths requires both a registry change and group policy change. You may need to consult your IT administrator for assistance making these changes.

Use the instructions in this section to enable long paths.

1. Press **Windows+R** on the keyboard. The Run dialog box displays.
2. Type `regedit`, and click **OK**. The Registry Editor window displays.
3. Using the expanding menu in the left-hand pane, navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem**.

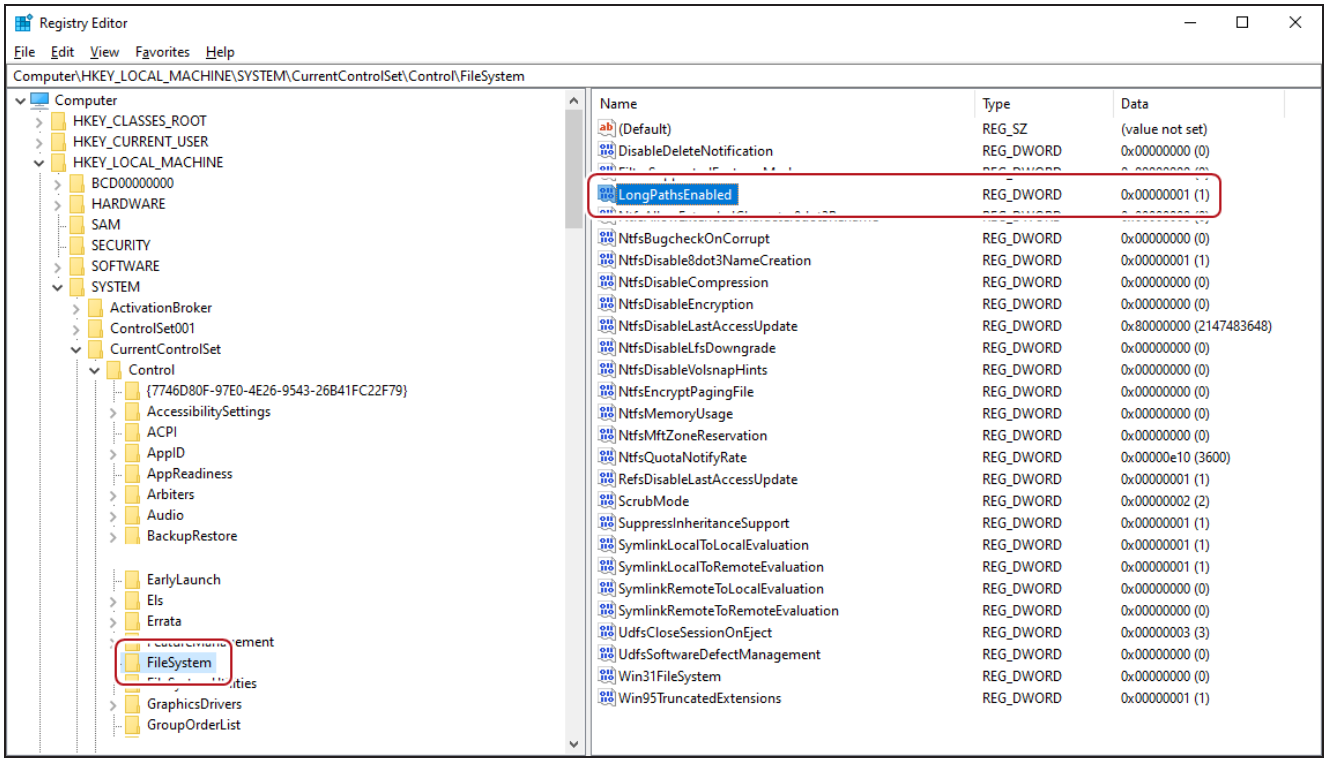


Figure 9 The Registry Editor window.

4. Right-click the **Filesystem** folder and select **New>DWORD (32-bit) Value**. A new value appears in the right-hand pane of the Registry Editor.
5. Enter `LongPathsEnabled` as the value name.

6. Double-click the **New Value**. The Edit DWORD (32-bit) Value dialog box displays.

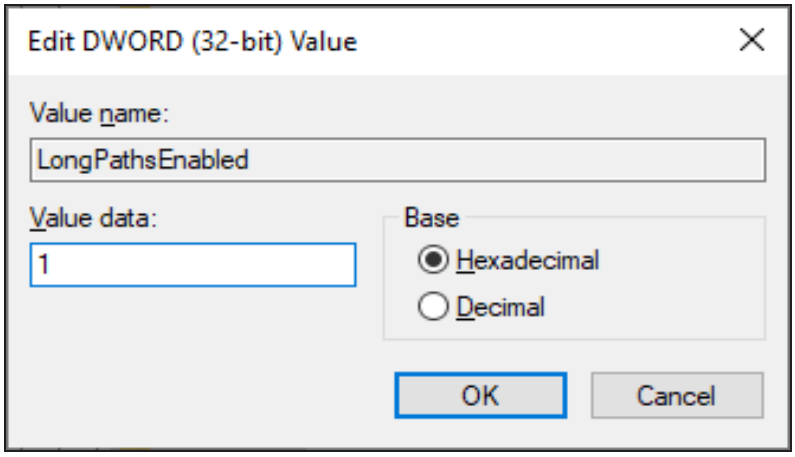


Figure 10 The Edit DWORD dialog box.

7. For **Base**, confirm **Hexadecimal** is selected.
8. Enter `1` in the **Value data** dialog box and click **OK**.
9. Select **File>Exit** to close the Registry Editor.
10. Press **Windows+R** on the keyboard. The Run dialog box displays.
11. Type `gpedit.msc`, and click **OK**. The Local Group Policy Editor window displays.

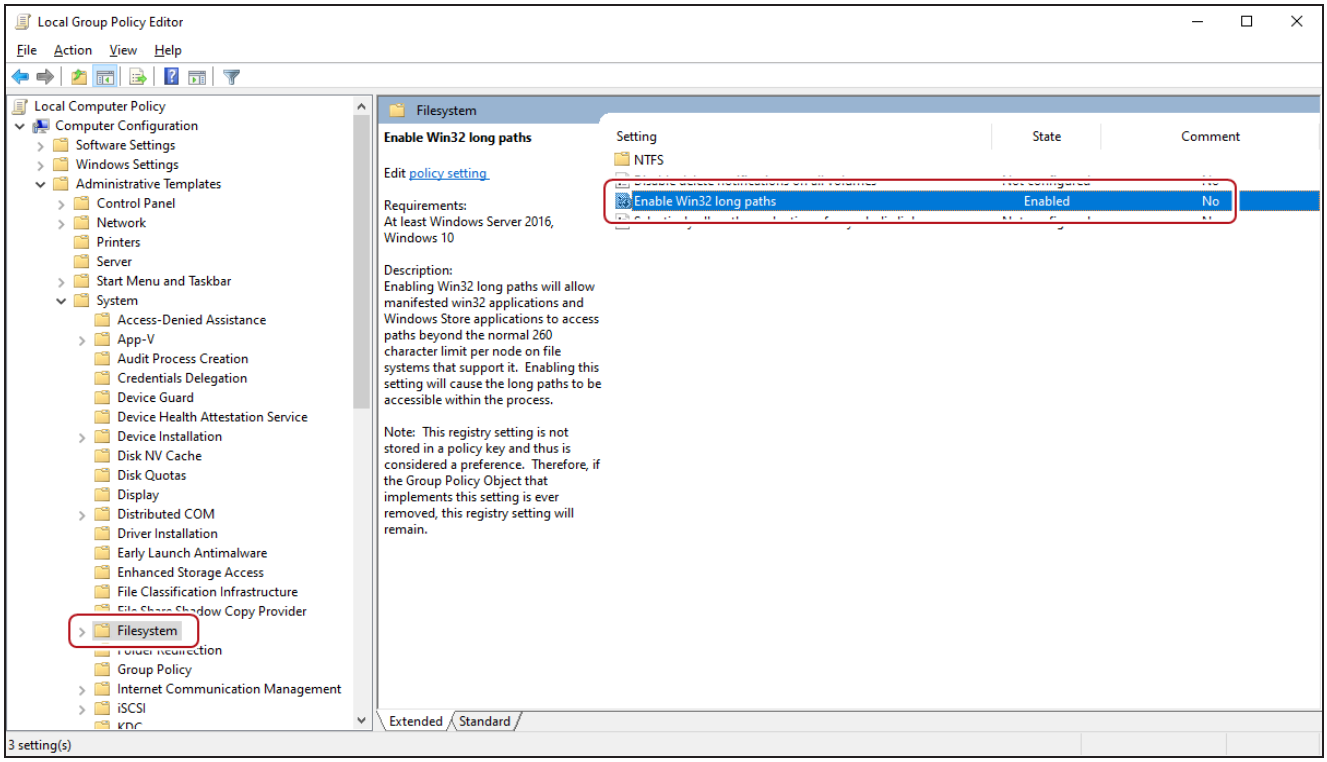


Figure 11 The Local Group Policy Editor window.

12. Using the expanding menu in the left-hand pane, navigate to **Computer Configuration>Administrative Templates>System>Filesystem**. The right-hand pane refreshes to display the filesystem options.
13. Double-Click **Enable Win32 long paths**. The Enable window displays.
14. Select **Enabled**, then click **OK**.

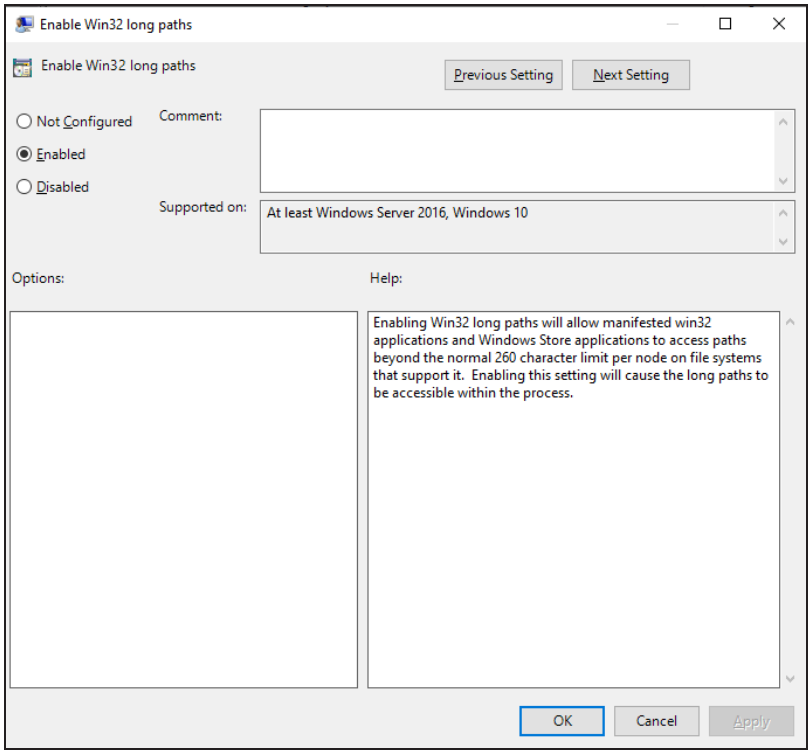


Figure 12 The Enable Win32 long paths dialog box.

15. Select **File>Exit** to close the Local Group Policy Editor.

Note: It may be necessary to reboot the Windows system after enabling long paths.

CONFIGURE FOR TRANSPARENT ACCESS

Replacing migrated / stored files with symbolic links allows transparent access to the files after they are moved to secondary storage.

IMPORTANT To use symbolic links, your source storage must support remote-to-remote symbolic links.

Enable Remote Symbolic Links

1. Open a Command Prompt as an Administrator.
2. To determine if symbolic link types are disabled, enter:

```
fsutil behavior query SymlinkEvaluation
```

3. If any symbolic link types report as disabled, enter the following:

```
fsutil behavior set SymlinkEvaluation L2L:1 R2R:1 L2R:1 R2L:1
```

DETERMINE SERVER UUID AND REQUEST A LICENSE

The StorCycle license is tied to the UUID of the StorCycle server. Use the following instructions to determine the UUID of the server.

1. On the StorCycle server, open a Command Prompt window.
2. Execute `wmic csproduct get "UUID"`. This returns a string representation of the UUID.
3. Send this UUID to Spectra Logic Technical Support (see Contacting Spectra Logic on page 9) for license generation.

Chapter 3 - Install the StorCycle Solution on a Linux Server

This section describes how to do an initial installation of the Spectra StorCycle Solution on a Linux server. For instructions to upgrade to a newer version of the Spectra StorCycle Solution see Upgrade the StorCycle Solution on page 244.

IMPORTANT

- The StorCycle solution runs on Windows servers and supports CIFS/SMB networked storage or runs on Linux servers and supports NFS-protocol storage or CIFS/SMB networked storage.
- If you are installing StorCycle on a Windows server, see Install the StorCycle Solution on a Windows Server on page 44.
- For instructions to upgrade to a newer version of the Spectra StorCycle Solution see Upgrade the StorCycle Solution on page 244.

VERIFY STORCYCLE REQUIREMENTS

Ensure that the server you will use for StorCycle meets the following minimum requirements:

Notes:
- Additional RAM and CPU cores will improve file transfer speeds in most cases.
- Customers are responsible for maintaining patches and upgrades on the operating system where StorCycle is installed.

- 64 GB RAM
- Four 64-bit CPU cores running at a minimum of 2.6 GHz
- 1 TB allocated to root
- 4GiB database drive space per 10 million files scanned/migrated.
- 10 GigE network or better
- Red Hat Enterprise Linux v8
- The installation user must have root privileges.
- A network which supports reverse DNS lookups. If the network does not support reverse DNS lookups, then the IPv4 address of the storage location is used in HTML links created during a migrate / store job. See Migrate / Store Wizard—Set Targets on page 174 for more information.
- The StorCycle solution uses whatever domain is configured on the server, including multiple / trusted domains, to access DNS (Domain Name System) to resolve UNC (Universal Naming Convention) paths over the domain and uses Active Directory / LDAP to verify restore users are valid on the domain.
- MongoDB requires a minimum of 4 GiB per 10 million files scanned/migrated. If files are versioned, each version is counted for database sizing.
- MongoDB must be supported by your operating system. For a compatibility matrix, see: *https://www.mongodb.com/docs/v5.0/administration/production-notes/*
- If BlackPearl storage locations are configured to group files into TAR or ZIP 'packs', the data to be packed is temporarily written to the server disk storage before it is transferred.
  - When using packing, the StorCycle solution requires enough server disk storage for ten times the size of a pack (10 * 10 GiB), or the largest file that will be migrated / stored in a pack, whichever is larger.
  - For maximum performance, Spectra Logic recommends that flash / SSD storage be used for the StorCycle server disk storage when creating TAR or ZIP packs.
  - Packing may use up to 500 GiB and the MongoDB will require (minimum) 4 GiB per 10 Million Files (assuming that no files being packed are larger than 10 GiB).
- The maximum file directory path length is 1024 characters.
- The user interface supports Google Chrome version 75 or later.

CONFIGURE VOLUME SNAPSHOTS FOR THE STORCYCLE DATABASE - LINUX

Before you can install the StorCycle solution, you must configure your system to create volume snapshots for the StorCycle database.

Use the instructions in this section to configure volume snapshots in a Linux environment.

Note: The below steps must be executed as a root user, or prefix commands with `sudo` as needed.

1. Enable thin pool and snapshot auto-extension

   ```
   vi /etc/lvm/lvm.conf
   ```

2. Within the **activation** section find or add these values:

   ```
   activation {
   ...
   thin_pool_autoextend_threshold = 70
   thin_pool_autoextend_percent = 20
   ...
   snapshot_autoextend_threshold = 70
   snapshot_autoextend_percent = 20
   ...
   }
   ```

3. Enable periodic block discards:

   ```
   systemctl enable --now fstrim.timer
   ```

4. Create a physical volume:

   a. Enter the following command:

      ```
      lsblk
      ```

      The command returns information similar to the following:

      ```
      NAME                    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
      nvme0n2                 259:4    0    68G  0 disk
      ```

b. Create a physical volume on the desired storage block devices listed in the previous step.

```
pvcreate /dev/block storage name
pvdisplay
```

The command returns information similar to the following:

```
"/dev/nvme0n2" is a new physical volume of "68.00 GiB"
--- NEW Physical volume ---
PV Name               /dev/nvme0n2
VG Name
PV Size               68.00 GiB
Allocatable           NO
PE Size               0
Total PE              0
Free PE               0
Allocated PE          0
PV UUID               513vL2-jDkN-mTUO-8YPj-d1qP-8pHN-xNplxv
```

5. Create the volume group:

```
vgcreate vg_mongo /dev/nvme0n2
vgdisplay
```

The command returns information similar to the following:

```
--- Volume group ---
VG Name               vg_mongo
System ID
Format                lvm2
Metadata Areas        1
Metadata Sequence No  1
VG Access             read/write
VG Status             resizable
MAX LV                0
Cur LV                0
Open LV               0
Max PV                0
Cur PV                1
Act PV                1
VG Size               <68.00 GiB
PE Size               4.00 MiB
Total PE              17407
Alloc PE / Size       0 / 0
Free  PE / Size       17407 / <68.00 GiB
VG UUID               KUAGVC-RLMM-ksnZ-gBAo-Olye-pdMW-xm8dJj
```

6. Create the logical volume:

```
lvcreate --size 1G --thin vg_mongo/mongo_pool --virtualsize
100G --name mongo_volume
```

```
lvs
```

The command returns information similar to the following:

```
mongo_pool    vg_mongo twi-aotz--   1.00g                0.00   11.04
mongo_volume  vg_mongo Vwi-a-tz-- 100.00g mongo_pool       0.00
```

7. Create the filesystem, mount, and enable mount on reboot:

```
mkfs.xfs /dev/vg_mongo/mongo_volume
```

```
mkdir /var/lib/mongo
```

```
mount /dev/vg_mongo/mongo_volume /var/lib/mongo
```

```
echo '/dev/vg_mongo/mongo_volume /var/lib/mongo xfs defaults 0
2' | tee -a /etc/fstab
```

8. Display the block information:

```
lsblk
```

The command returns information similar to the following:

```
NAME                      MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
nvme0n2                   259:4    0    68G  0 disk
├─vg_mongo-mongo_pool_tmeta   253:9    0     4M  0 lvm
│ └─vg_mongo-mongo_pool-tpool 253:11   0     1G  0 lvm
│   ├─vg_mongo-mongo_pool     253:12   0     1G  1 lvm
│   └─vg_mongo-mongo_volume   253:13   0   100G  0 lvm  /var/lib/mongo
└─vg_mongo-mongo_pool_tdata   253:10   0     1G  0 lvm
  └─vg_mongo-mongo_pool-tpool 253:11   0     1G  0 lvm
    ├─vg_mongo-mongo_pool     253:12   0     1G  1 lvm
    └─vg_mongo-mongo_volume   253:13   0   100G  0 lvm  /var/lib/mongo
```

9. Create a test snapshot:

```
lvcreate --name mongo_snap_test --snapshot /dev/vg_mongo/mongo_
volume
```

10. Verify the test snapshot creation:

```
lvdisplay /dev/vg_mongo/mongo_snap_test
```

The command returns information similar to the following:

```
--- Logical volume ---
LV Path                /dev/vg_mongo/mongo_snap_test
LV Name                mongo_snap_test
VG Name                vg_mongo
LV UUID                jM92vZ-45ZO-p5CT-hfRc-kAJ5-u1Qk-UY2iKJ
LV Write Access        read/write
LV Creation host, time localhost.localdomain, 2024-10-05 15:38:27 -0700
LV Pool name           mongo_pool
LV Thin origin name    mongo_volume
LV Status              NOT available
LV Size                100.00 GiB
Current LE             25600
Segments               1
Allocation             inherit
Read ahead sectors     auto
```

11. Delete the test snapshot:

```
lvremove /dev/vg_mongo/mongo_snap_test
```

CREATE THE STORCYCLE MONGO DATABASE REPOSITORY

MongoDB Version Compatibility Chart

The StorCycle application requires the MongoDB application to work correctly. Before checking or creating the MongoDB repository, use the table below to determine what version of MongoDB is required for the version of the StorCycle solution you are installing.

StorCycle Version Number	MongoDB Version Number
3.7.0	MongoDB 4.0
3.7.1	MongoDB 4.0
4.0.0	MongoDB 4.2
4.1.0	MongoDB 4.4
4.2.0	MongoDB 5.0
4.3.0	MongoDB 6.0

Check for an Existing MongoDB Repository

Your environment may already have the correct MongoDB repository installed on your system. Use the commands below to check if a MongoDB repository exists and if it is the correct version.

1. Confirm connectivity to the MongoDB server:

   ```
   ping repo.mongodb.org -c 4
   ```

2. Check the version of the MongoBD repository:

   ```
   yum repolist | grep mongo
   ```

3. Do one of the following:

   - If a MongoDB repository is installed, confirm it is the correct version using the table in MongoDB Version Compatibility Chart above. If the repository is the correct version, continue with Install the StorCycle Solution on page 70.

     -OR-

   - If a MongoDB repository is not installed, or it is not the correct version, continue with Create the MongoDB Repository on the next page

Create the MongoDB Repository

IMPORTANT

Do not install MongoDB directly for your Linux installation. Instead you must create the repo file for the unique MongoDB version that matches that StorCyle version. After creation, the repo file is renamed and edited to allow StorCycle to pull down the proper MongoDB version and install the Mongo database automatically during the StorCycle solution installation.

The following instructions provide an example using Yum to create the Mongo Database Repository.

Note: Do not use these instructions when **upgrading** the StorCycle software. There are additional steps when upgrading, see Upgrade the StorCycle Solution on page 244.

The following instructions are for **installing StorCycle 4.3.0**. If you are installing a different version of the software, you need to adjust the values in red below to the appropriate version. The StorCycle solution requires a specific MongoDB version that is compatible with the version of StorCycle. See MongoDB Version Compatibility Chart on the previous page to determine the required MongoDB version for your StorCycle solution version.

1. Open the terminal and sign in as a superuser.
2. Create a file with the following name:

   ```
   /etc/yum.repos.d/mongodb-org-6.0.repo
   ```

3. Open the file and enter the following:

   ```
   [mongodb-org-6.0]
   name=MongoDB Repository
   baseurl=https://repo.mongodb.org/yum/redhat/releaseversion/mongodb-org/6.0/x86_64/
   gpgcheck=1
   enabled=1
   gpgkey=https://www.mongodb.org/static/pgp/server-6.0.asc
   ```

INSTALL THE STORCYCLE SOLUTION

The StorCycle.rpm file is delivered as a link from a Spectra representative. Move the .rpm file to the server where you plan to install the StorCycle solution. Complete all Configure Volume Snapshots for the StorCycle Database - Linux on page 64 and Create the StorCycle Mongo Database Repository installation steps before running the .rpm StorCycle file.

1. Navigate to the directory in which the .rpm file is located or give the full path to the file. The .rpm must run as root.
2. To install the StorCycle .rpm, use the following command:

   ```
   sudo yum install -y ssc-production-X.X.X.XXX.XXXXXXXX.rpm
   ```

3. If desired, change the user from root using the following commands (where *user* and *group* refer to the user you want to change):

   ```
   sudo chown -R user:group /var/lib/ssc
   sudo vi /usr/lib/systemd/system/ssc.service
   # User=root - change root to the new user name
   sudo setcap CAP_NET_BIND_SERVICE=+eip /sbin/ssc
   sudo systemctl restart ssc
   ```

START, STOP, AND RESTART THE SERVICES

To check if the services are running, execute the following commands.

MongoDB: `sudo systemctl status mongod`

StorCycle: `sudo systemctl status ssc`

To start the mongod or StorCycle processes, issue the appropriate command below.

MongoDB: `sudo systemctl start mongod`

StorCycle: `sudo systemctl start ssc`

To stop the mongod or StorCycle processes, issue the appropriate command below.

MongoDB: `sudo systemctl stop mongod`

StorCycle: `sudo systemctl stop ssc`

To restart the mongod or StorCycle processes, issue the appropriate command below.

MongoDB: `sudo systemctl restart mongod`

StorCycle: `sudo systemctl restart ssc`

MOUNT LINUX STORAGE DEVICES

Prior to configuring NAS storage in the StorCycle solution, mount the storage device(s) using the following commands.

1. Create a directory.

   ```
   sudo mkdir ./mount-point
   ```

2. Mount the share to the created directory.

   For NFS shares, use the following:

   ```
   sudo mount -t nfs server:/directory /mount-point
   ```

   For CIFS shares, use the following:

   ```
   sudo mount -t cifs -o
   username="user",password="password",domain="domain",iocharset=utf8,
   dir_mode=0755 //uncpath/to/share /mount-point
   ```

   Note: In order for users to use symbolic links to access files in secondary storage, the share must be mounted on the StorCycle Linux server using the same mount point used by all users of the primary storage. For example, if users of the primary storage mount 'nas_server/share1' as 'mnt/share1', then the StorCycle server must also mount it as 'mnt/share1'. If the StorCycle server instead uses a different mount point, symbolic links created by the StorCycle solution will not provide access to the file.

3. Mount any desired read-only shares to the directory.

DETERMINE SERVER UUID AND REQUEST A LICENSE

The StorCycle license is tied to the UUID of the StorCycle server. To get the UUID of the server, execute the following command in a shell:

```
cat /etc/machine-id
```

Send this UUID to Spectra Logic Technical Support (see Contacting Spectra Logic on page 9) for license generation.

Chapter 4 - Start Using the StorCycle Solution

This section describes how to get started using the Spectra StorCycle Solution after completing the installation (see Install the StorCycle Solution on a Windows Server on page 44 or Install the StorCycle Solution on a Linux Server on page 62).

User Interface Overview

The user interface provides browser-based configuration, management, and monitoring of the Spectra StorCycle solution. The following sections describe the common features that appear in all screens in the user interface.

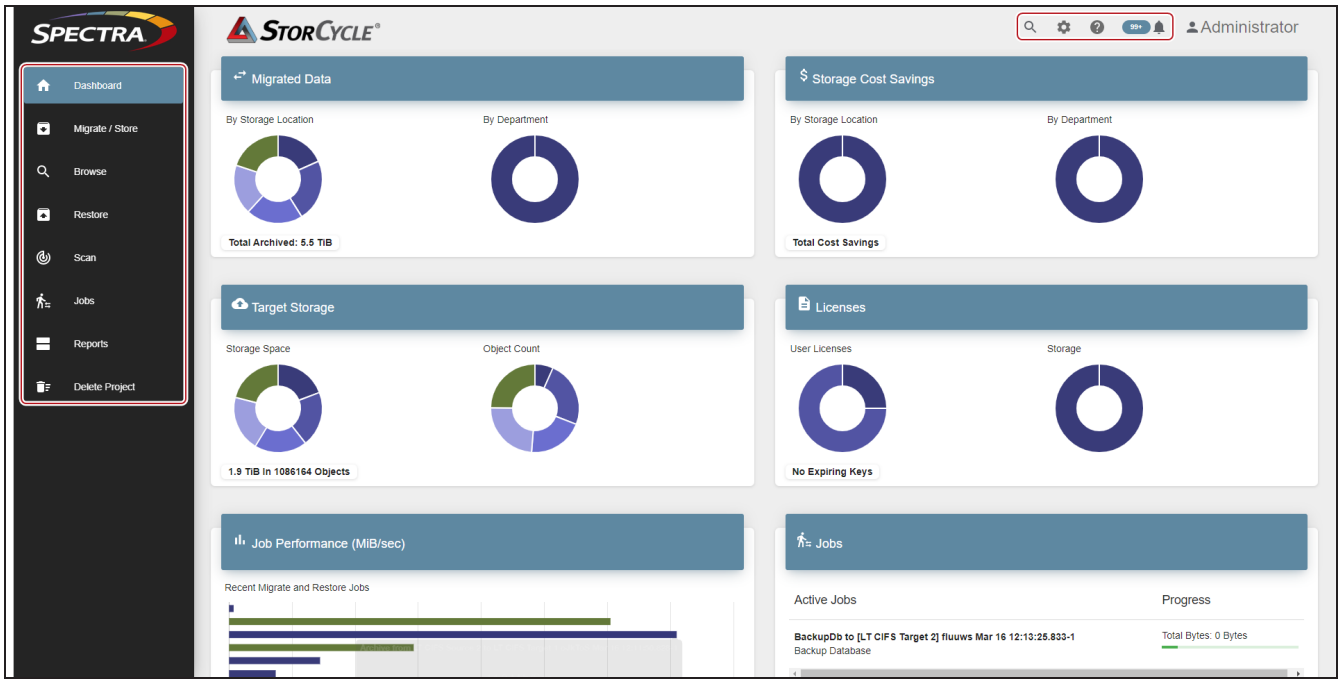


Figure 13 The Dashboard screen of the Spectra StorCycle solution user interface.

Taskbar

The taskbar displays along the left edge of each screen. The following table provides an overview of the selections in the taskbar.

Taskbar	Description
Dashboard	The **Dashboard** navigation link returns you to the Dashboard screen from any other screen in the interface. The Dashboard screen displays the amount of data migrated, the target storage used, the cost saving for all migrated / stored data, licensed storage, active and queued jobs, job performance, and the cumulative scan data for each source storage location.
Migrate / Store	The **Migrate / Store** navigation link takes you to the Migrate / Store screen which displays configured migrate / store projects and job statuses and provides access to the wizard for configuring new migrate / store projects. See Migrate or Store Data on page 164 for more information.

Taskbar	Description
Browse	The **Browse** navigation link takes you to the Browse screen which displays a search menu and provides access to the wizard for configuring new restore projects from the search results. See Restore and Browse Objects on page 187 for more information.
Restore	The **Restore** navigation link takes you to the Restore screen which displays configured restore projects and job statuses and provides access to the wizard for configuring new restore projects. See Restore and Browse Objects on page 187 for more information.
Scan	The **Scan** navigation link takes you to the Scan screen which displays configured scan projects and job statuses and provides access to the wizard for configuring new scans. See Scan on page 149 for more information.
Jobs	The **Jobs** navigation link takes you to the Active and Completed Jobs screen which displays information about active and completed jobs. See Jobs on page 230 for more information.
Reports	The **Reports** navigation link takes you to the Reports screen which displays links to the following reports: • Settings and Configuration — Configuration information, such as software version; Users; Departments; Storage Location settings; Projects. • Jobs and Status — Logs; Migrate / Store, Restore, and Scan Jobs; Scans and Data Analysis; Data Transfer; Catalogs (list); Cost Savings by Department; System Messages; Delete Jobs. • Catalogs — List of migration / store catalogs. Click **Details** to see the name, description, created time, updated time, type, created by, and project name information for the catalog. Click **List** to see a list of objects included in the catalog and the original path for the file. Buttons on each displayed report allow saving it in CVS or JSON format. See Reports on page 237 for more information.
Delete Project	The **Delete Project** navigation link takes you to the Delete Project screen which provides an interface for deleting all of the files migrated / stored by a project. See Delete Project on page 184 for more information. **Note:** The **Delete Project** link is only available for Administrator or Cypto Officer users.

Toolbar

The toolbar displays in the upper right corner of each screen.

The following table provides an overview of the selections in the toolbar.

Icon	Meaning	Description
	**Search**	Takes you to the Search screen used to search the catalog for files to restore. See Search for Project on page 193 for more information.

	**Settings**	**Note:** The Settings menu is only available to Administrator or Crypto Officer users.
		It provides access to the Settings menu which allows you to configure or view the following:
		• Configuration
		  • Active Directory / LDAP
		  • Departments
		  • Global Settings
		  • Licenses & SSL Certificate
		  • SMTP
		  • Users
		• Database Backup
		• Encryption - An encryption password can only be configured by a Crypto Officer
		• Linked Instances
		• Logs
		• Storage
		• BlackPearl
		See Storage on page 81 and Required Settings on page 127 for more information.

	**Help**	Displays the help system.
	**Messages**	**Note:** The Messages menu is only available to Administrator or Crypto Officer users. Displays the messages generated by the Spectra StorCycle solution. The messages are categorized as: • **Info** - An expected event occurred such as a job starting or completing successfully.

Icon	Meaning	Description
		• **Warning** - A job completed with warnings or errors, for example, a file to be migrated / stored was already migrated / stored, therefore, it was skipped. Determine the cause of the problem and remedy it if necessary. • **Error** - A job failed with warnings or errors, for example, the StorCycle solution cannot communicate with a storage location. Determine the cause of the error and remedy it as soon as possible.
	**User**	Indicates the user currently logged in and provides access to the Logout function.

Other Icons

The table below describes icons that display on various screens in the user interface.

Icon	Meaning	Description
	Actions Drop Down	Displays all actions possible for the corresponding storage location or migrate / store project.
	**Cancel**	Click to cancel a queued, verifying, or active job.
	**Clone**	Click to duplicate a previous migrate / store project with a new name or to create a new BlackPearl storage location using the same endpoint and credentials of an existing location.
	**Delete / Disable**	Click to delete jobs or logs, or to disable projects.
	**Delete Files**	Click to delete files.
	**Details**	Click to display details. On a message details screen, you can also mark the message as read.
	**Download**	Click to download logs. See Logs on page 241.

Icon	Meaning	Description
	**Edit**	Click to edit a migrate / store project, storage location, department, or user.
	**Ingest**	Click to have the StorCycle solution ingest the data in the bucket associated with the BlackPearl target to manage it.
	**List**	Click to see the listing of items in a catalog.
	**Pause / Disable**	Click to pause the schedule for a project or disable the project.
	**Refresh**	Click to refresh the jobs listing. **Note:** The Refresh icon displays on several background colors.
	**Restore**	Click to restore the object in the catalog search.
	**Resume / Disable**	Click to resume the schedule for a project or disable the project.
	**Run**	Run a recurring or single-run migrate / store, database backup, or scan project.
	**Savings Calculator**	Click to open the Savings Calculator section of a Scan Job Details screen. See Savings Calculator on page 235 for more information.
	**Send Test Email**	Click to send a test email to the associated user.
	**View Details**	Click next to a storage location to view details about the storage location.

Supported Browsers

The user interface supports Google Chrome version 75 or later, on Windows, macOS, and Linux.

LOG INTO THE USER INTERFACE

Use one of the following methods to log into the Spectra StorCycle solution user interface.

- If you created a desktop shortcut during the installation process, double-click the shortcut to launch the StorCycle user interface.
- Using a supported web browser (see Supported Browsers on the previous page), do one of the following:
  - If you are on the server, enter `https://localhost` and press the Enter key.
  - If you are on a host on the same network as the server, enter the IP address for the Spectra StorCycle solution server with the https: port (for example `https://xxx.xxx.xxx.xxx/app`) and press the Enter key.

Note: You must include `https://`.

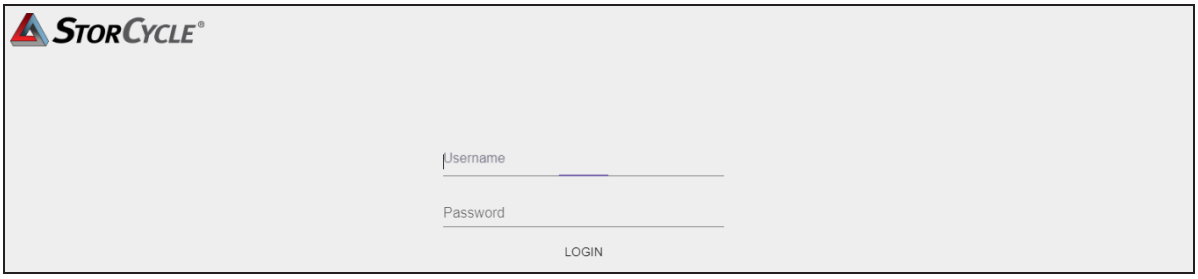


Figure 14 The Spectra StorCycle solution Login screen.

1. Enter the **Domain** for a Domain User or clear the **Domain** for a Non-Domain User.

Note: This field only displays when Active Directory / LDAP is configured.

2. Enter the primary administrator username and password.

   The default username is **administrator**. The default password is **spectra**.

Notes:
- Usernames are case insensitive.
- Spectra Logic recommends that you change the default password for the primary administrator (see Configure Users on page 142).

3. Click **Login** to log in. The remainder of this guide assumes that you are logged in to the Spectra StorCycle solution user interface.

IMPORTANT

After five unsuccessful login attempts, a local user is locked out and the password must be reset by an administrator. See Reset a Local User Password on page 224 for instructions.

Active Directory user login attempts follow Active Directory policies. To protect the Active Directory server, the Spectra StorCycle solution adds a 1 second delay on the next login attempt for every invalid login attempt.

LOAD LICENSE KEYS

License keys enable features and capacity within the Spectra StorCycle solution.

Use the instructions below to load new license keys.

1. Click **Settings** in the toolbar and then select **Configuration > Licenses & SSL Certificate**. The Licenses & SSL Certificate screen displays showing any licenses currently installed in the software.

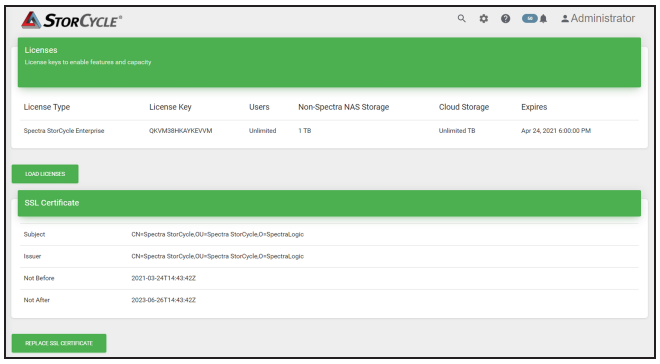


Figure 15 The Licenses & SSL Certificate screen.

2. Click **Load Licenses**. The Load Licenses dialog box displays.

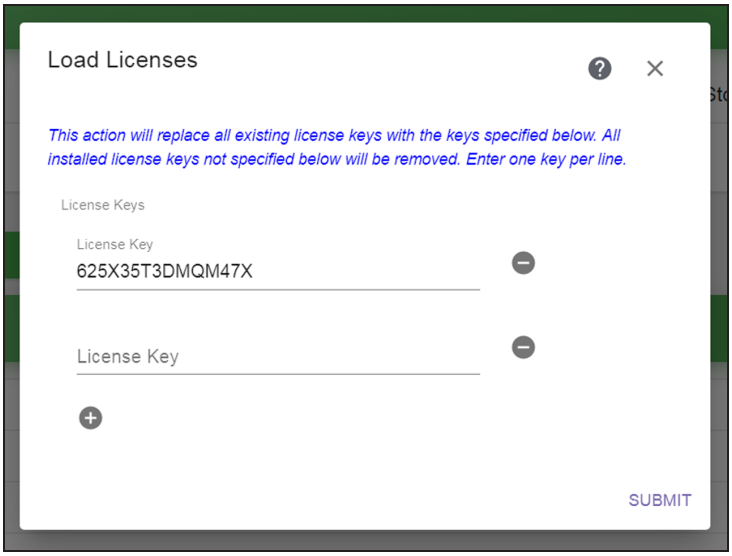


Figure 16 The Load Licenses dialog box.

3. Click the minus (-) sign next to any license that you want to remove.
4. Click the plus (+) sign to add a new line for entering a license. Enter all license keys, exactly as provided, one per line.
5. Click **Submit** to save the license keys. The Licenses & SSL Certificate screen displays with the newly entered keys listed.

NEXT STEPS

To begin using your StorCycle solution, follow the user guide as it progresses through the general steps outlined in the checklist below.

	Operation	Description
☐	**Add License Keys**	License keys are required to use the StorCycle solution. See Load License Keys on the previous page.
☐	**Configure Storage**	Configure both source and target storage locations. See Configuring Storage on page 89.
☐	**Configure Database Backup**	Configuring a daily database backup job is critical to the use of the StorCycle solution and is required for any migrate job which removes or replaces source data. See Database Backup on page 128.
☐	**Configure Global Settings**	Global settings control aspects of the solution that are important to configure before beginning to process data. See Configure Global Settings on page 135.
☐	**Configure Active Directory / LDAP**	If your StorCycle environment uses Active Directory or LDAP, it is important to configure it before using the StorCycle solution. See Configure Active Directory / LDAP on page 137.
☐	**Configure Users**	Optional. However it is best practice to configure all required users before using the StorCycle solution. See Configure Users on page 142.
☐	**Configure SMTP**	Configuring SMTP allows you to receive emails with system messages generated by the solution and is highly recommended by Spectra Logic. See Configure SMTP on page 147.
☐	**Configure Other Settings**	Optional. Features such as encryption, SSL certificates, linked instances, and other optional settings can be configured now or later depending on the requirements of your storage environment. See Other Settings and Features on page 209
☐	**Configure a Scan Project**	Configure a scan project to evaluate data in primary storage. See Create a Scan Project on page 157.
☐	**Begin Storage Operations**	Once the above steps are completed, you are ready to begin data storage operations.

Chapter 5 - Storage

This section provides instructions for configuring and working with storage locations. Configure both source (primary storage) and target (secondary storage) storage locations before configuring a migrate / store project. You must also create storage before configuring database backups.

STORAGE LOCATION BEST PRACTICES

To monitor the cost savings from migrating from the Primary Storage Tier to the Perpetual Storage Tier, for each storage location enter a department (see Configure Departments on page 220) and a cost per terabyte (TiB). StorCycle will then monitor the amount of data moved between storage locations and calculate an associated cost savings.

The use of local storage (for example \\localhost\c$) for source or target storage locations is not supported.

Source Storage Location Best Practices - General

Note: A BlackPearl gateway cannot be configured as a source storage location.

StorCycle Storage Locations that are sources of data (data to be migrated) can be configured to be at the top-level directory of a storage server share or at a sub-directory lower down in the directory structure path.

Consider the following when deciding where to place the StorCycle source Storage Locations:

- Do the directories contain data for different departments or groups and is tracking of storage usage and cost by department/group desired? If so, each department/group should have its own Storage Location.
- Are there different pools of data that will have different methods of being scanned or archived? For example, some data may need to be scanned weekly whereas other data never needs to be scanned. Or, one pool of data may be archived manually by project or directory, whereas another pool of data is automatically archived on a scheduled basis based on the age of the data. If these different types of pools of data exist, then each should have their own Storage Location.

Source Storage Location Best Practices - NAS Storage

When creating a NAS share on a Windows host, several permissions are inherited by the share. If a permission does not already exist on the Windows host, it is created.

Inherited permissions from archive and restore target directories may conflict with permissions StorCycle attempts to archive or restore from the original source objects and directories. When permissions conflict, the operation may generate warnings, errors, and may make changes to file accessibility. Typically these permissions are CREATOR_OWNER, CREATOR_GROUP, AND EVERYONE.

Spectra Logic recommends disabling inheritance for both archive and restore target directories as described below. This allows the StorCycle solution to preserve the existing permissions of the source object during archive and restore operations.

Note: BlackPearl NAS source storage does not support symlinks.

When creating a new NAS share, configure the share with the following permissions:

- Local Administrators - Full Control - This folder, files and subfolders.
- SYSTEM - Full Control - Full Control - This folder, files and subfolders.
- If you created a custom StorCycle user, set the permission to StorCycle Service Account - Full Control - This folder, files and subfolders.
- Inheritance should be disabled by clicking "Disable Inheritance".
- Remove all other permissions.

Versioning

When versioning is enabled, multiple versions of a file from the source storage location are kept on the target storage location after multiple migrate / store jobs. Each file name has a code appended to the file name that indicates the date and time that the migrate / store job started, in the format `yyyymmddhhmmss` using a 24-hour clock using UTC time. Versioning can be configured on a per source storage location basis to create versions for all files in the source or only files that changed, and to keep a set number of versions of a file, deleting the oldest when necessary.

Notes:

- HTML and Symbolic Links are not supported in Migrate / Store jobs from versioned sources.
- If a versioned source is used in multiple projects, Spectra Logic recommends that each project uses a different working directory.
- When packing is enabled on a target, and a versioned source is used with **keep XX versions**, the StorCycle solution is not able to delete older versions from the target. If a job is restored from a target with packing enabled and which contains a versioned file which has been deleted due to **keep XX versions**, the StorCycle solution does not include the deleted file in the restore, even if it still exists in a pack. The deleted version does not exist in the StorCycle database and the restore job completes without warnings or errors.
- The StorCycle solution assumes that all files with the exact same file name and directory path are the same file for versioning, and determines change criteria based on file size and hash. If a versioned file is removed from a source location, and then replaced with a different file with an identical file name, the StorCycle solution continues versioning the new file with the identical file name as if it was an edited version of the old file.
- The StorCycle solution does not track content to determine which version of the file is current. If an older version of the file is restored to the source and then archived again, it is now considered the newest version of the file.

Configuring Versioning

Configuring versioning is a step in the configuration process for all types of source storage location. See Configuring Storage on page 89.

IMPORTANT Spectra Logic recommends that a versioned source is only used in one migrate / store project at a time.

Versioning cannot be disabled for an existing source after a migrate / store job from the source is used, and it cannot be enabled for an existing source that was previously used.

Changed Files Only option - If selected, a new version is created only when the file changes (file modified time and hash changes). If not selected a new version is created whenever there is a migrate / store job from the source storage location. The **Changed Files Only** option can be enabled or disabled at any time.

Versions to Keep option - If selected, the StorCycle solution keeps the specified number of versions on the target storage location. Each day at midnight UTC, the StorCycle solution determines the number of versions of a file on target storage locations and automatically deletes the oldest copies if there are more than specified. If not selected, versions are not automatically deleted. This option is compatible with both standard versioning and **Changed Files Only** versioning. The **Versions to Keep** option can be enabled or disabled at any time.

Note: When a versioned file is deleted from a target, the associated job is updated to remove information about the file so that an attempt to restore the file cannot occur.

IMPORTANT **Versions to Keep** applies to all projects associated with a source location. If two independent projects are using the same source to two different targets, the StorCycle solution will maintain XX versions across all projects. For example, if the storage location is configured to keep 3 versions and Project A has already created 3 versions, after Project B migrates / stores the same source to a different target, the StorCycle solution will automatically remove a version from Project A's target.

Storage Location Security

To add storage location security to a new or existing source storage location, an administrator can assign an AD / LDAP group to the source storage location which restricts access to scan, migrate / store, and restore jobs, as well as file listings associated with the source, to members of the designated group and administrators. If AD / LDAP is not configured, access is restricted to administrators. The StorCycle solution queries the AD / LDAP server if a user attempts to configure a new restore job to or scan or migrate / store job from the controlled source. For recurring jobs (scans and migrate / stores), the StorCycle solution queries the domain server each time it attempts to initiate the job.

The StorCycle solution also queries the server when a user tries to access information regarding a job to / from a controlled source, such as the Catalog File Listings. The StorCycle solution does not query the AD / LDAP server when assigning groups to source locations, so groups can be assigned without the domain server configured and non-existent groups can be assigned.

Configuring storage location security is a step in the configuration process for all types of source storage location. See Configuring Storage on page 89.

Notes:
- Spectra Logic recommends that top level domain groups (not nested groups) be created specifically for the use of managing StorCycle access. Due to the complexity of domain groups, heavily nested groups may introduce search query issues for the StorCycle solution. The AD/LDAP settings include a search query which will be used to query the domain server and will assist in some nested group searches.
- Modifications to the AD/LDAP group search query should only be performed by system administrators who have an understanding of the organizations domain settings.
- StorCycle supports the configuration of only a single domain server and only a single AD group can be assigned to a source location.

What is Restricted - StorCycle Administrators are never restricted. If a Storage Manager or Restore User is not a member of the configured source domain group, they will not be able to perform the following actions:

- Scans on controlled source storage locations
- Migrate / store jobs from controlled sources
- Restore jobs which came from the controlled sources
- Restore jobs to the control sources (which originated from another source)
- (continued on next page)

- Viewing of catalog file listings associated with the controlled source

Notes:
- If a group is assigned to a source that does not actually exist on the domain, the StorCycle solution allows the configuration, but only administrators are able to access the source.
- If a group is assigned but an AD / LDAP domain is not configured, only administrators have access to the source.
- Job details, such as job completion and job statistics are not restricted for any user.
- File names are visible in warnings and error messages.
- Access permission determination occurs when the job starts, so that any changes in group membership are taken into account.

Job ownership - Within the Job Details page for scans, migrate / stores, and restores, the StorCycle solution lists the 'Created By' user. This is the user whose permissions are assessed during recurring jobs. If a job is edited, a new field is present in the Job Details called 'Updated By'. If an Updated By user exists, the StorCycle solution uses this user's group memberships to assess permissions.

Target Storage Location Best Practices

StorCycle Storage Locations that are targets for migrated data can be configured to be at the top-level directory of a storage server share, at a sub-directory lower down in the directory structure path, or to buckets depending on the storage type.

Consider the following when deciding the StorCycle target Storage Locations to create:

- To avoid potential directory and file name conflicts on the target, create enough unique target Storage Locations so that data from multiple storage location sources is not migrated / stored to the same storage location targets (buckets or directories). For example, if source Storage Locations A and B both contain a top-level directory **dir1** which contains a file **file1.txt**, and the file from both locations are migrated to the same target, there could be an error or a re-write of data due to both storage locations having data with the same file path and file name.
- The StorCycle solution should be the only application / user using the target storage path (Spectra NAS, non-Spectra NAS, S3, or BlackPearl system).
    - You should not modify files once they are on the target. If a file is changed on the target after being migrated / stored, a restore using the StorCycle solution will fail due to a checksum error.
    - You should not add or remove files, folders, or objects from a target storage location
- If the target is a BlackPearl system or cloud storage location, make sure the target is using versioning to avoid migrate / store job failures. See the *Spectra BlackPearl Converged Storage System User Guide* for details.
- If the target is a Spectra or non-Spectra NAS storage location, you can select different sub-directories to avoid the conflict.

Encryption Best Practices

The StorCycle solution supports single key encryption for all storage targets. The key is saved in memory. If the server reboots, the password must be reentered.

CAUTION Safely store the encryption password. If you lose the encryption password, you are not able to access the data stored by the StorCycle solution after a server reboot.

IMPORTANT Once encryption is enabled and the encryption password is set, it cannot be disabled and the password cannot be changed.

IMPORTANT StorCycle encryption does not protect the file name and metadata information on the target.

IMPORTANT Only users with a Crypto Officer role can enable or disable encryption. See Configure Users on page 142 for more information about different user types.

Note: Using encryption may have a performance impact on the server CPU.

Retention Policy Best Practices

Note: Retention policies are only supported for data center and enterprise licenses.

A storage location retention policy allows you to select the desired number of days to retain files on a storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery.

- Spectra Logic recommends that the root of a target is never used for a storage location with a retention policy.
- When adding a retention policy to an existing target storage location, any existing Symbolic or HTML links may be broken when the retention policy runs.
- Audit files for retention policy / deletes are stored in a StorCycle system directory (C:\Program Files\Spectra Logic Corporation\Spectra StorCycle\audit or $HOME/.ssc/audit) which should be backed up regularly.
- Pending Delete notifications should be enabled for all Administrator users.
- Pending delete notifications are sent approximately five days before the delete occurs. Retention policies that are less than 5 days do not generate warning emails ahead of time.
- Spectra Logic recommends never changing a Retention policy after it is configured, to prevent unintended deletion of data.
- Targets which are using a retention policy should utilize a specific naming scheme to help administrators and users understand which targets have retention policies.

Spectra NAS Snapshot Best Practices

When configuring a Spectra NAS storage location, you can select to **Enable Snapshot** to create a snapshot after a migrate / store job, a retention policy delete, or a delete files job using this target location.

Notes:

- A volume configured for snapshots must already exist on the Spectra NAS system.
- Existing storage locations which have been used in a job can have snapshots enabled and will begin taking snapshots with the next migrate / store job.
- For maximum protection from ransomware, the Spectra NAS volume should be configured for read-only and should not be used by any user or application besides the StorCycle solution – no data should be added, modified, or deleted from this volume outside of the StorCycle solution.
- As a best practice, only a single Spectra NAS storage location should be configured per volume.
- If a Spectra NAS volume is shared by multiple StorCycle Spectra NAS storage locations, all locations must be configured with either read / write or read-only.
- A snapshot is taken even when no objects are sent by a job, or the job fails.
- Snapshots are managed and restored by the Spectra NAS system.

CAUTION Restoring to an earlier snapshot on the volume leads to loss of data (and access) from the StorCycle solution. Migrate / store operations following the restore point will no longer be restore-able from the StorCycle solution.

CONFIGURING STORAGE

Storage consists of both source and target storage locations. Source storage data is scanned and archived to target storage using migrate / store jobs. Restore jobs move data from target storage back to the source storage location.

Supported Source Storage - NAS, S3, Google Cloud

Support Target Storage - Spectra BlackPearl NAS, non-Spectra NAS, S3, AWS, Microsoft Azure, Google Cloud

IMPORTANT The StorCycle solution runs on Windows servers and supports CIFS/SMB networked storage or runs on Linux servers and supports NFS-protocol storage or CIFS/SMB networked storage.

Notes:

- Storage locations cannot be deleted after they are used in a project, but can be hidden from the Storage screen. See Retire/Delete a Storage Location on page 125 or more information.
- You cannot configure a storage location to use encryption before encryption is configured or the encryption password is re-entered after a server reboot. See Enable Encryption on page 210 for more information.
- To clone a current BlackPearl storage location, see Clone a BlackPearl Storage Location on page 120.
- To ingest data from a BlackPearl bucket, see Ingest Data in BlackPearl Bucket on page 123.

Use the instructions below to configure a new storage location.

1. Click **Settings** in the toolbar and then select **Storage**. The Storage screen displays showing all storage locations currently configured in the software.

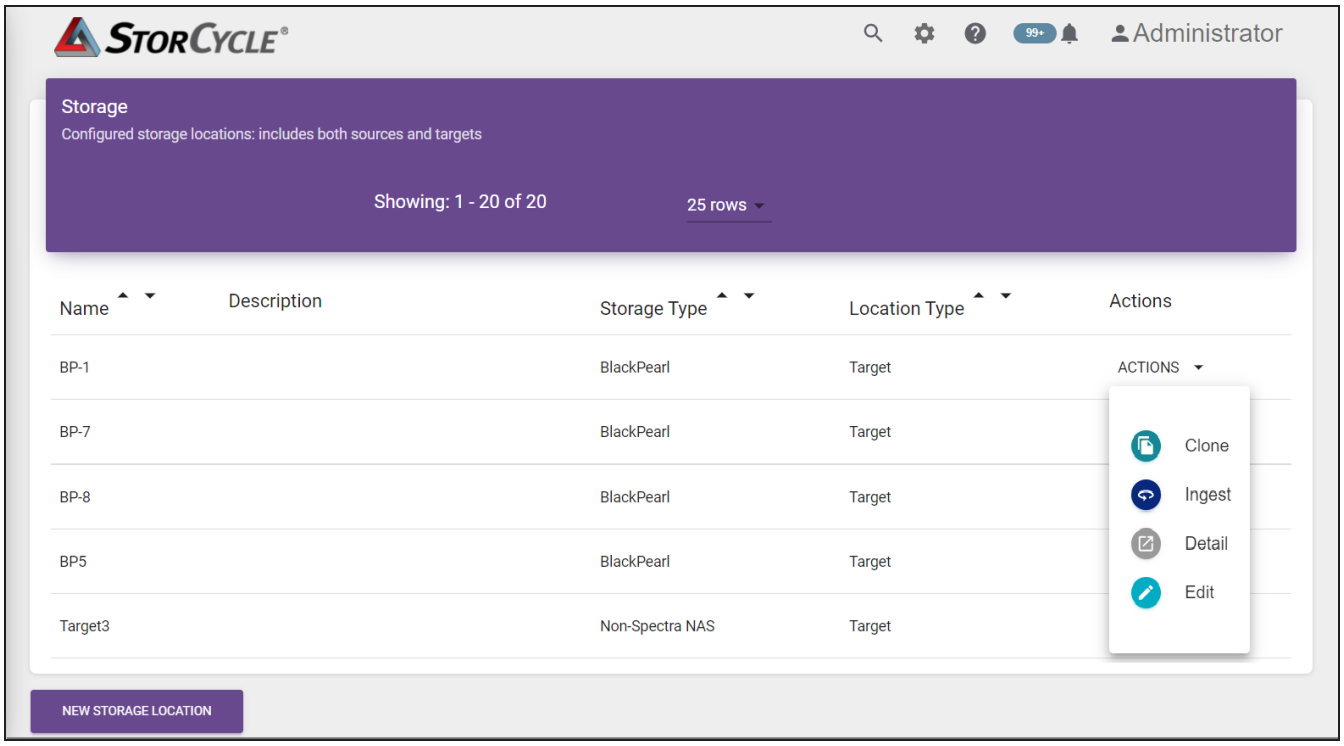


Figure 17 The Storage screen.

2. Click **New Storage Location**. The New Storage Location dialog box displays.

Note: If you are creating a new BlackPearl storage location and want to use the same endpoint and credentials of an existing BlackPearl storage location, see Clone a BlackPearl Storage Location on page 120.

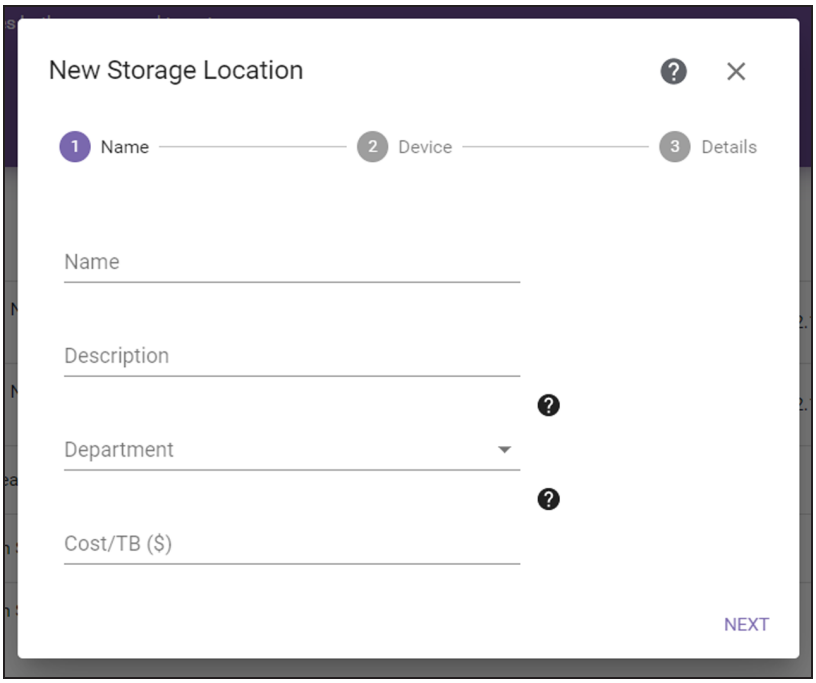


Figure 18 The New Storage Location dialog box.

3. Enter a unique **Name** for the storage location.
4. If desired, enter a **Description** for the storage location.
5. If desired, use the drop-down list to select the **Department** responsible for the storage location costs. To create a department, see Configure Departments on page 220.
6. If desired, enter the **Cost/TiB** to use for storage location costs. Do not enter the currency symbol.

Note: See Configure Global Settings on page 135 to change the currency.

7. Click **Next**. The New Storage Location Device dialog box displays.

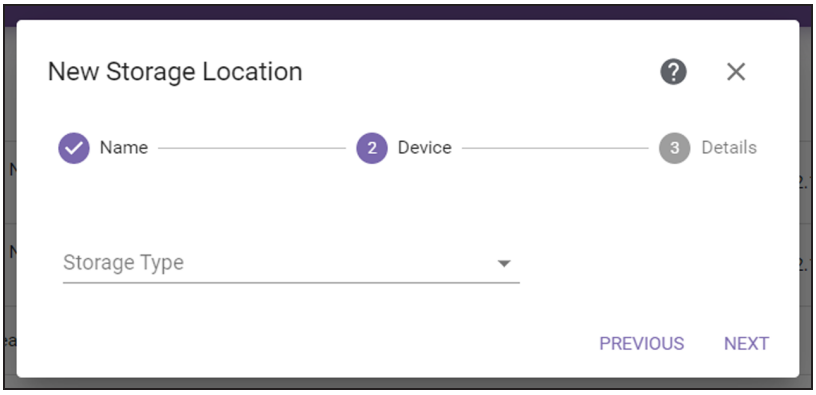


Figure 19 The New Storage Location Device dialog box.

8. Use the drop-down list to select the **Storage Type**.

   Continue with the applicable section below:

- Enter BlackPearl Storage Location Information on the next page
- Enter Spectra NAS Storage Location Information on page 97
- Enter Non-Spectra NAS Storage Location Information on page 104
- Enter S3 Storage Location Information on page 110
- Enter Microsoft Azure Storage Location Information on page 114
- Enter Microsoft Azure Archive Storage Location Information on page 117

Enter BlackPearl Storage Location Information

IMPORTANT See "Understanding Spectra Advanced Bucket Management Concepts" in the *Spectra BlackPearl Converged Storage System User Guide* for information about configuring data placement policies for a bucket to meet your archiving needs and for instructions to gather the information to configure the storage location.

Note: BlackPearl storage locations can only be target locations.

If you select the **BlackPearl** storage type, the dialog box updates to display the following:

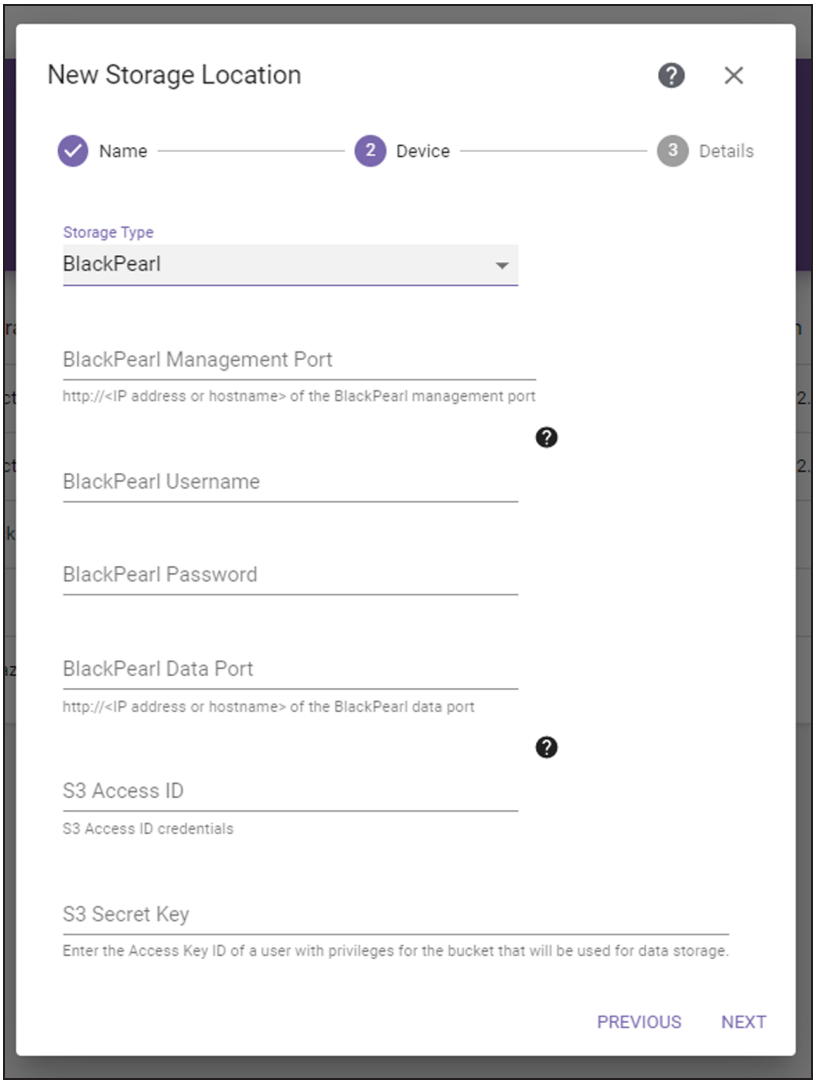


Figure 20 The New Storage Location BlackPearl Device dialog box.

1. Enter the IP address or hostname for the **BlackPearl Management Port**. Include http://.

2. Enter the **Username** of a BlackPearl user with **only** Login and Monitor permissions. If the BlackPearl system has Active Directory configured, the user must also have Active Directory administrator permission. The user **cannot** have Administrator or SpectraApp permissions.

   Note: Spectra Logic recommends dedicating this user to the StorCycle solution and not assigning the user to other data storage operations.

3. Enter the **Password** associated with the username entered above.
4. Enter an IP address or hostname for the **BlackPearl Data Port**. Include http://.
5. Enter the **S3 Access ID** of a user with credentials for the BlackPearl system and the bucket that will be used for data storage.
6. Enter the **S3 Secret Key** associated with the **S3 Access ID** entered above.

   Note: The S3 Access ID and Secret Key are found on the User Details screen in the BlackPearl user interface.

7. Click **Next**. The BlackPearl Storage Location Details dialog box displays.

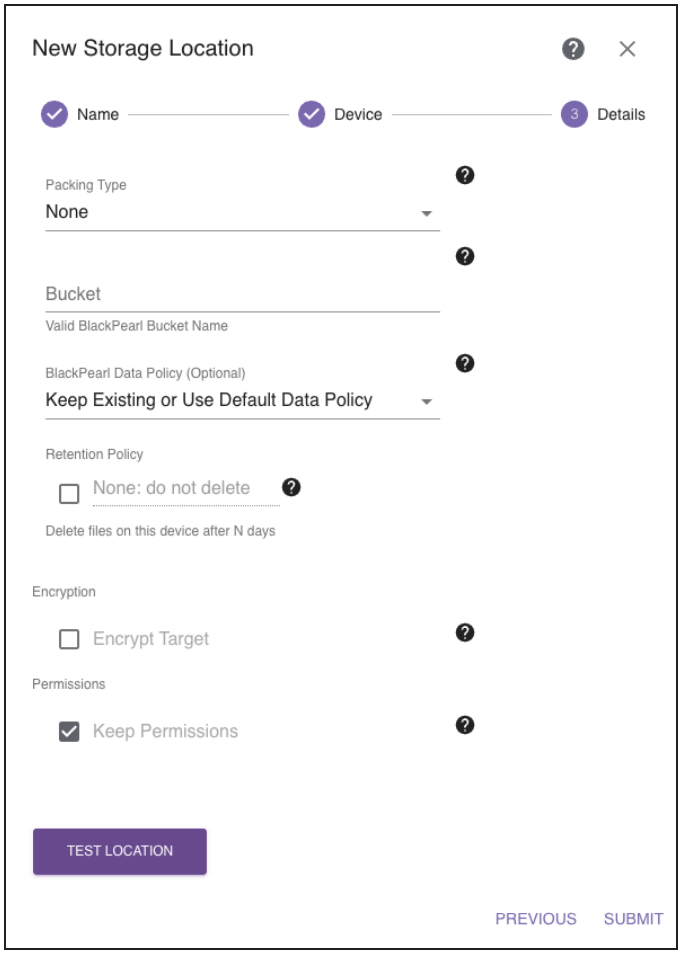


Figure 21 The New Storage Location BlackPearl Details dialog box.

8. Select whether archived data should be packed into larger files for transfer, and, if so, which **Packing Type** to use.

   When migrating many small files, packing improves performance by reducing the total number of objects that are migrated and managed by the BlackPearl system. This also reduces the total size of the BlackPearl database. Individual files in packs are tracked by StorCycle, and users may restore a single or multiple individual files which are stored in a pack.

   StorCycle packs can be accessed outside of the StorCycle solution using a tool to unzip or untar the packed file.

Notes:
- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files are added to packs until the pack reaches 10,000 files or reaches 10 GiB of data.
- Files are never split between packs.
- Up to five packs can be created at the same time.

9. Enter the name of the **Bucket** to be used for data storage. If the bucket does not exist, it is created.

CAUTION Make sure the target bucket uses a data policy with versioning enabled to avoid migrate / store jobs failing if a file with the same name already exists in the bucket.

Note: Bucket names must meet the following criteria:
- Bucket names must be at least 1 character long and not more than 63 characters long.
- Bucket names must not contain special characters such as @, $, #, %, {, }, or |.
- Spectra Logic recommends following AWS bucket naming conventions. For more information, go to: https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html

10. Do one of the following:
    - If the bucket already exists, you can select **Keep Existing or Use Default Data Policy** or **View Existing Bucket Policy** to see the data policy assigned to the bucket.

      -OR-

    - If the bucket is new, you can select **Keep Existing or Use Default Data Policy** or **Specify Policy on New Bucket**, then use the **Data Policy** drop-down menu to select an existing data policy.

11. If desired, select the **Retention Policy** check box and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87 for more information.

Notes:
- Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.
- When the storage location is configured to use packing, files deleted by retention are not removed from the packs, but are removed from the StorCycle database and cannot be restored.

12. If desired, select the **Encrypt Target** check box to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted. See Enable Encryption on page 210 for more information.

Note: Only users with a Crypto Officer role can enable or disable encryption.

13. If desired, select **Keep Permissions** to preserve file permissions on the storage location.
14. Click **Test Location** to verify that the server can connect to the storage location. If the StorCycle solution does not return a check mark indicating it can communicate with the storage location, you must resolve the error before submitting the location.
15. Click **Submit** to save the storage location.

Enter Spectra NAS Storage Location Information

Before adding the NAS storage location to the StorCycle solution, Spectra Logic recommends configuring NAS share permissions as described in Source Storage Location Best Practices - NAS Storage on page 82

IMPORTANT The StorCycle solution requires that a Spectra NAS system be running BlackPearlOS 5.1.2 or later.

If you select the **Spectra NAS** storage type for a Spectra BlackPearl NAS or Verde system, the dialog box updates to display the following fields:

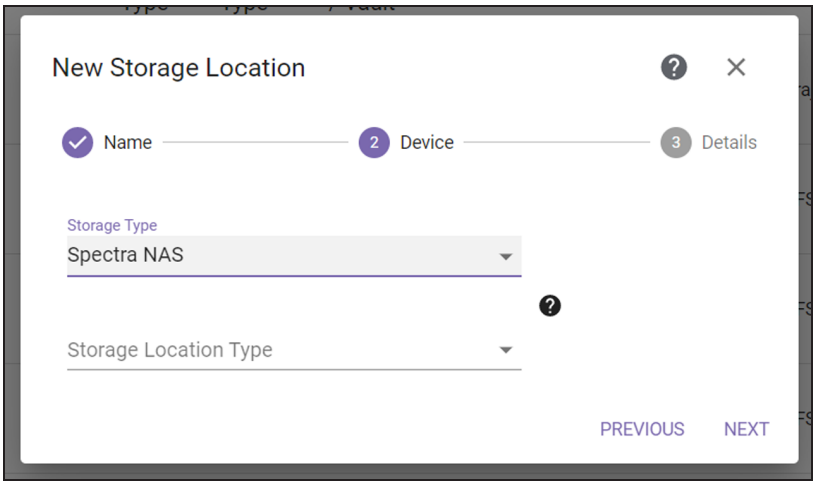


Figure 22 The New Storage Location Spectra NAS Device dialog box.

1. For **Storage Location Type**, select whether the storage location will act as a **Source** or a **Target**.
2. Click **Next**. The Spectra NAS Storage Location Details dialog box displays. The options that display are different if you are creating source or target storage. First you configure settings common to both types of storage, then use either the source or target storage instructions depending on the type of storage you are configuring.

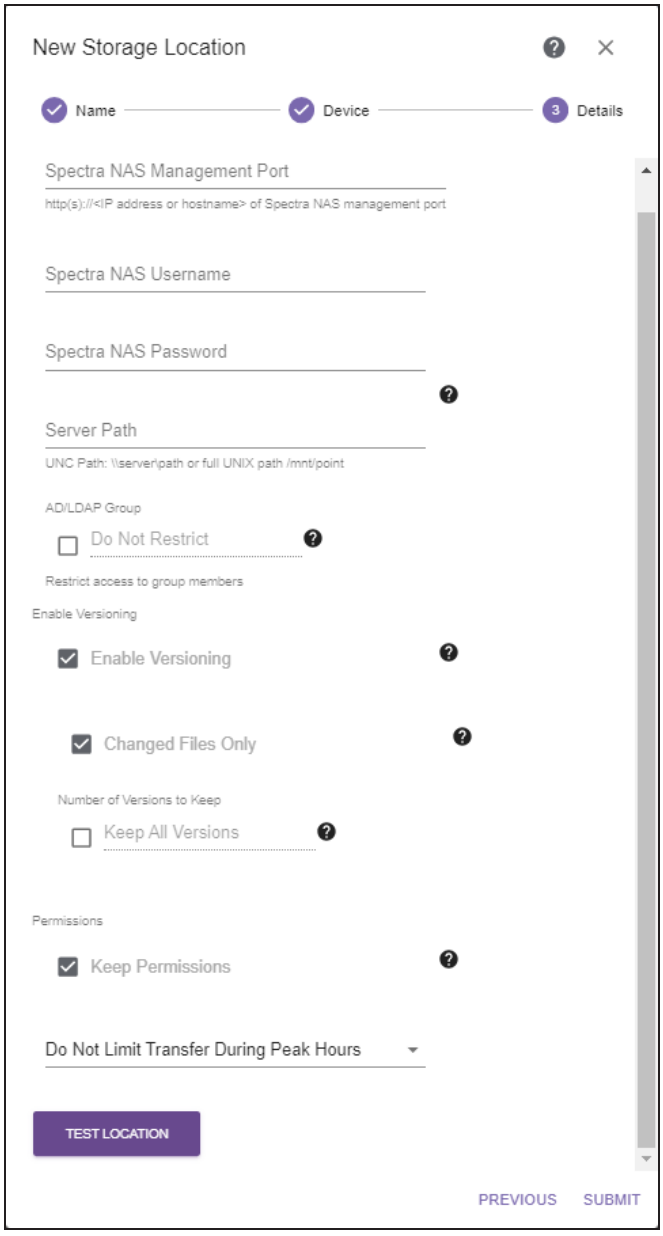


Figure 23 The New Storage Location Spectra NAS **Source** Details dialog box.

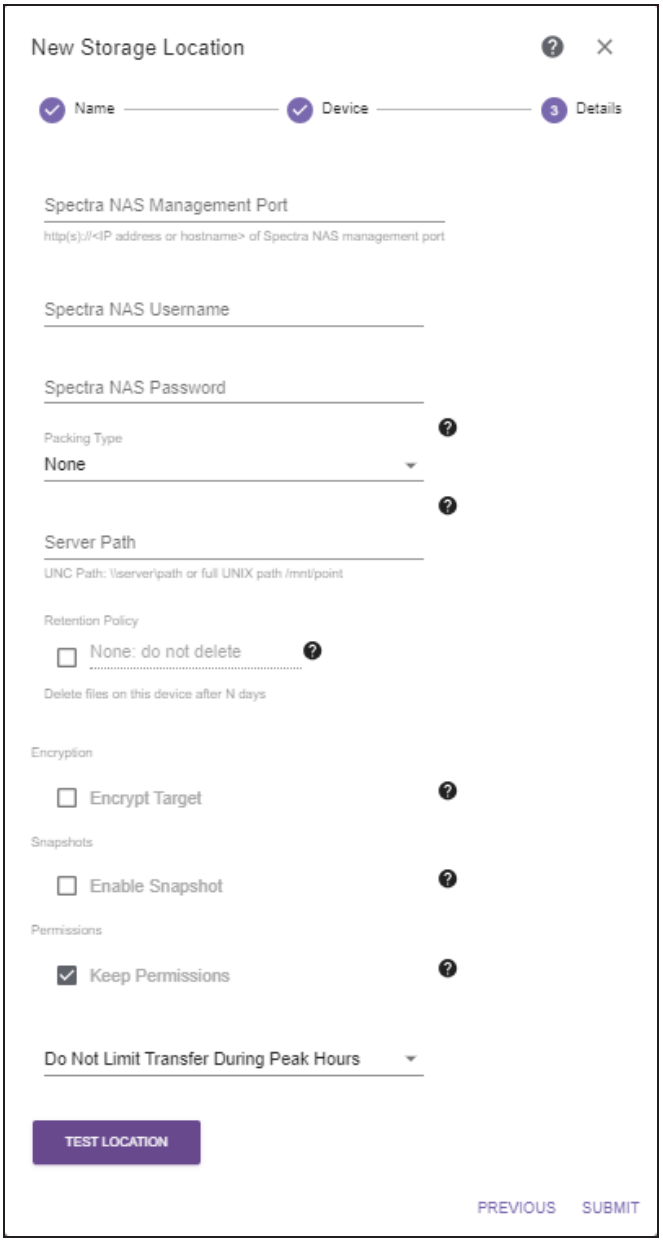


Figure 24 The New Storage Location Spectra NAS **Target** Details dialog box.

Steps for Both Storage Types

1. Enter the IP address or hostname for the **Spectra NAS Management Port**. Include http://.

   Note: The Spectra NAS Management Port, and Spectra NAS Username and Password are used to authenticate that this is Spectra NAS for licensing purposes.

2. Enter the **Spectra NAS Username** of a user with Login user access as well as Monitor and/or Administrator user access, or if the Spectra NAS system has Active Directory configured, an Active Directory administrator.

   Note: If the BlackPearl solution has multi-factor authentication enabled, the user must have Monitor and Login access, and not Administrator access.

3. Enter the **Spectra NAS Password** associated with the username entered above.
4. Enter the file system **Server Path** to the NAS mount point (\\server\path or full UNIX path /mnt/point).

IMPORTANT

Storage location server paths should not overlap. For example:

- The storage location server path should not be a sub-directory of an existing storage location path.
- The storage location server path should not have as a sub-directory an existing storage location path.
- The storage location server path cannot be the same as an existing storage location path with different capitalization.

IMPORTANT The server path name should not be the same as a BlackPearl bucket that you plan to ingest. See Ingest Data in BlackPearl Bucket on page 123 for more information.

5. Continue with either the **source storage** or **target storage** instructions below:
   - Steps for Source Storage below

     -OR-

   - Steps for Target Storage on the next page

Steps for Source Storage

1. If desired, select **AD / LDAP Group** and enter an AD / LDAP group to restrict access to scan, migrate / store, and restore jobs, as well as file listings associated with the source, to members of the designated group and administrators. If you select this option and AD / LDAP is not configured or the entered user group does not exist, access is restricted to administrators. See Storage Location Security on page 84 for more information.
2. If desired, select **Enable Versioning** to keep multiple versions of a file from the source storage location on the target storage location after multiple migrate / store jobs. See Versioning on page 83 for more information.
3. If you selected **Enable Versioning**, select whether to create versions for **Changed Files Only**.
4. If you selected **Enable Versioning**, select whether to limit the number of **Versions to Keep** and if so, enter or select the number to keep.
5. Continue with Next Steps for Both Storage Types on page 101.

Steps for Target Storage

1. Select whether archived data should be packed into larger files for transfer, and which **Packing Type** to use. When migrating many small files, packing improves performance by reducing the total number of objects that are migrated and managed. This also reduces the total size of the database. Individual files in packs are tracked by StorCycle, and users may restore a single or multiple individual files which are stored in a pack. StorCycle packs can be accessed outside of the StorCycle solution using a tool to unzip or untar the packed file.

Notes:
- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files are added to packs until the pack reaches 10,000 files or reaches 10 GiB of data.
- Files are never split between packs.
- Up to five packs can be created at the same time.

2. If desired, select **Retention Policy** and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87 for more information.

Note: Retention policies are only supported for data center and enterprise licenses.

3. If desired, select **Encrypt Target** to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted.

Note: Only users with a Crypto Officer role can enable or disable encryption.

4. If desired, select **Enable Snapshot** to create a snapshot after a migrate / store job, a retention policy delete, or a delete files job using this target location.

Notes:
- For maximum data protection, Spectra Logic recommends enabling snapshots.
- A volume configured for snapshots must already exist on the Spectra NAS system.
- The Spectra NAS volume should not be used by any user or application besides the StorCycle solution – no data should be added, modified, or deleted from this volume outside of the StorCycle solution.
- A snapshot is taken even when no objects are sent by a job, or the job fails.
- Snapshots are managed and restored by the Spectra NAS system.

CAUTION Restoring to an earlier snapshot on the volume leads to loss of data (and access) from the StorCycle solution. Migrate / store operations following the restore point are no longer able to be restored from the StorCycle solution.

5. If you selected **Enable Snapshot**, select **Keep Volume Read Only** to configure the StorCycle solution to set the NAS volume to read-only after a migrate / store job completes. When selected, before sending data to this target, the StorCycle solution sends a 'pre' command to set the target to read / write, performs a migrate / store job, sets the target to read-only, and then takes a snapshot of the volume. This provides ransomware protection, but is only suitable for a storage location dedicated to data from StorCycle migrate / store jobs.

Notes:
- For maximum protection from ransomware, the Spectra NAS volume should be configured for read-only.
- As a best practice, only a single Spectra NAS storage location should be configured per volume on the Spectra NAS system.
- If a Spectra NAS volume is shared by multiple StorCycle Spectra NAS storage locations, if one storage location is configured to generate snapshots and to keep the NAS volume read-only, any additional storage locations targeting that volume must also be configured to keep the NAS volume read-only.

6. Continue with Next Steps for Both Storage Types below.

Next Steps for Both Storage Types

1. If desired, select **Keep Permissions** to preserve file permissions on the storage location.
2. Use the drop-down menu to select either:
   - Do Not Limit Transfer During Peak Hours below
   - Limit Transfer During Peak Hours below

Do Not Limit Transfer During Peak Hours

If you selected **Do Not Limit Transfer During Peak Hours**, continue with Test and Submit the Storage Location on page 104.

Limit Transfer During Peak Hours

If you selected **Limit Transfer During Peak Hours**, the configuration options for limiting transfer display.

Note: Limiting transfer during peak hours only applies when reading from the storage location. If the Storage Location Type is Source, this occurs when the location is scanned or is the source of a migrate / store project. If the Storage Location Type is Target, this occurs when a restore is done of a file previously migrated / stored to the target.

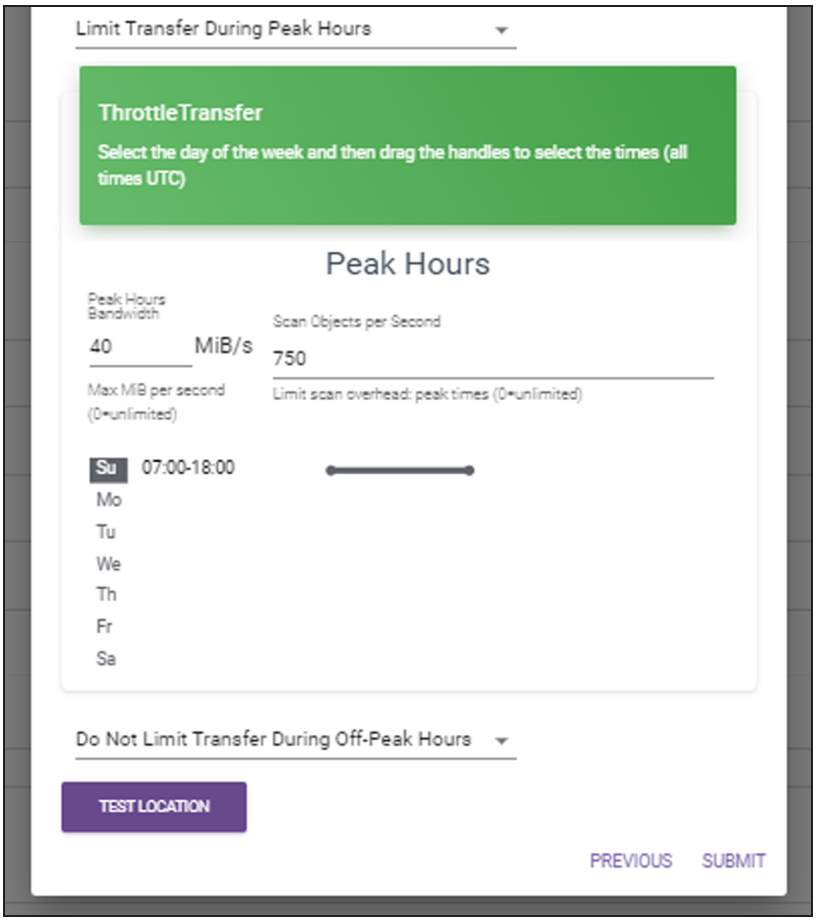


Figure 25 The Limit Transfer During Peak Hours configuration settings.

a. Enter the **Peak Hours Bandwidth**. The default is 40 MiB/s. Spectra Logic recommends starting with 10% of peak load and then adjust as necessary by editing the storage location.

b. Enter the maximum **Scan Objects per Second** during peak hours. The default is 750.

c. Select a day of the week for which you want to designate peak hours. The default peak hour selection of 07:00-18:00 (7:00 AM - 6:00 PM) displays. Select and move a handle to change the start and end times. Repeat this step for other days as necessary.

Note: The time range is in Coordinated Universal Time (UTC), not local time.

d. Use the drop-down menu to select either **Do Not Limit Transfer During Off-Peak Hours**, or **Limit Transfer During Off-Peak Hours**, and follow one of the sections below.

3. Use the drop-down menu to select either:

- Do Not Limit Transfer During Off-Peak Hour on the next page
- Limit Transfer During Off-Peak Hours on the next page

Do Not Limit Transfer During Off-Peak Hour

If you selected **Do Not Limit Transfer During Off-Peak Hours**, continue with Test and Submit the Storage Location on the next page.

Limit Transfer During Off-Peak Hours

When you selected **Limit Transfer During Off-Peak Hours**, the configuration options for limiting transfer display.

Note: Limiting transfer during off-peak hours only applies when reading from the storage location. If the Storage Location Type is Source, this occurs when the location is scanned or is the source of a migrate / store project. If the Storage Location Type is Target, this occurs when a restore is done of a file previously migrated / stored to the target.

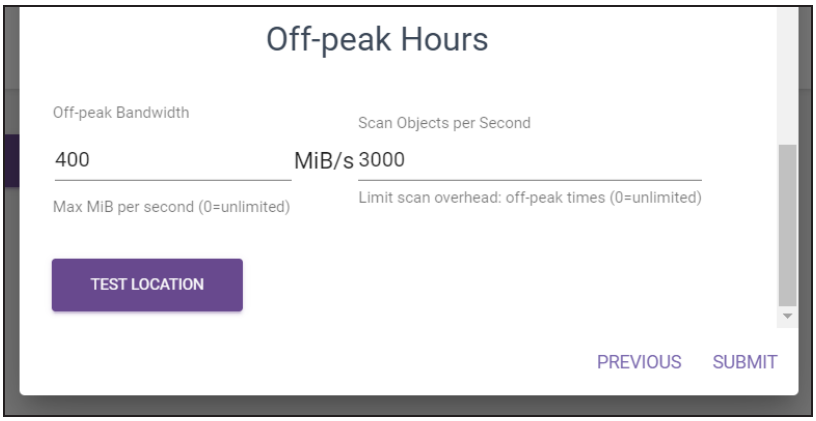


Figure 26 The Limit Transfer During Off-Peak Hours configuration settings.

a. Enter the **Off-Peak Bandwidth**. The default is 400 MiB/s. Spectra Logic recommends starting with 100% of peak load and then adjust as necessary by editing the storage location.

b. Enter the maximum **Scan Objects per Second** during off-peak hours. The default is 3000.

c. Continue with Test and Submit the Storage Location on the next page.

Test and Submit the Storage Location

1. Click **Test Location** to verify that the server can connect to the storage location. If the StorCycle solution does not return a check mark indicating it can communicate with the storage location, you must resolve the error before submitting the location.

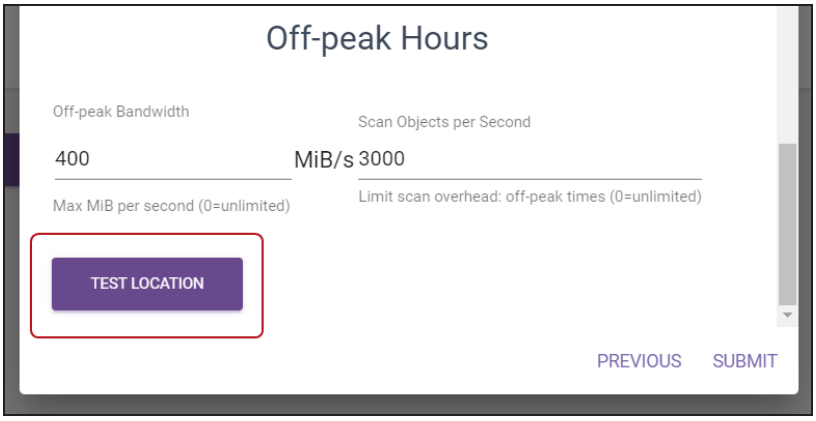


Figure 27 The Test Location button.

   If the test is successful, a check mark displays to the right of the Test Location button.

2. Click **Submit** to save the storage location.

Enter Non-Spectra NAS Storage Location Information

Note: If you enter a BlackPearl NAS system or Verde NAS system as a Non-Spectra NAS storage location, it will count against the Non-Spectra NAS storage access limit for licensing. See Licensing on page 42 for more information.

If you select the **Non-Spectra NAS** storage type, the dialog box updates to display the following fields:

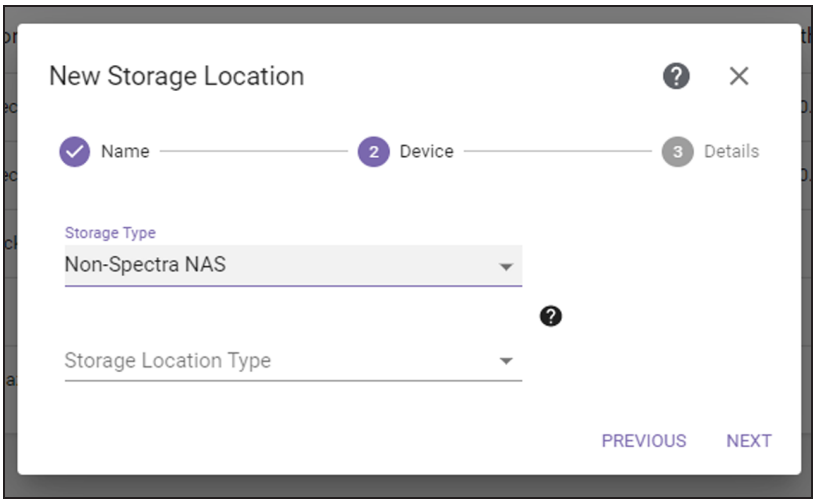


Figure 28 The New Storage Location Non-Spectra NAS Device dialog box.

1. For **Storage Location Type**, select whether the storage location will act as a **Source** or a **Target**.
2. Click **Next**. The Non-Spectra NAS Storage Location Details dialog box displays.

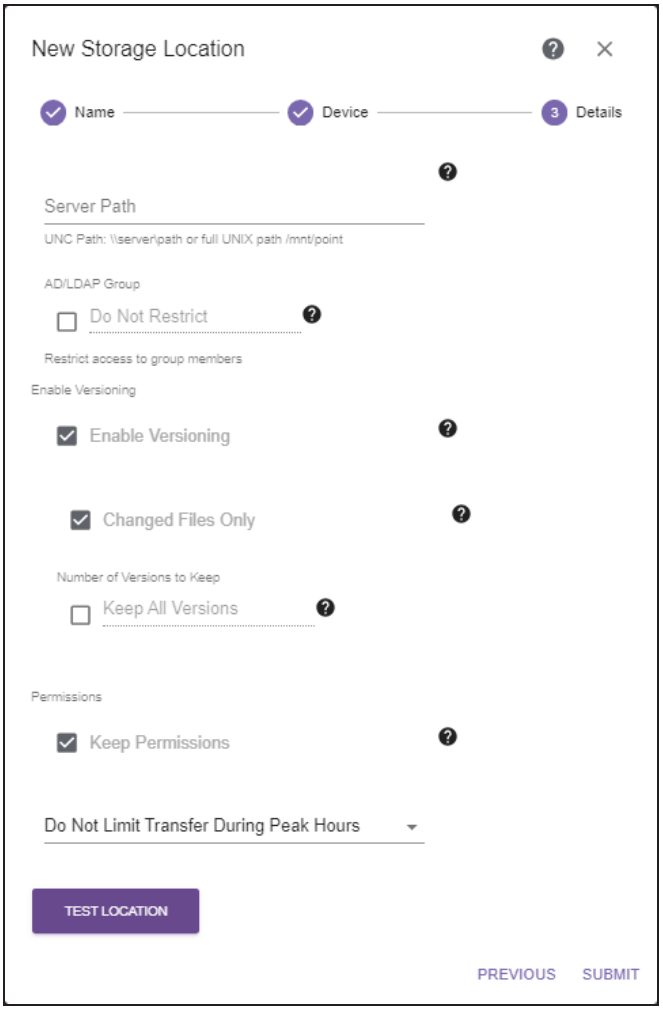


Figure 29 The New Storage Location Non-Spectra NAS Source Details dialog box.

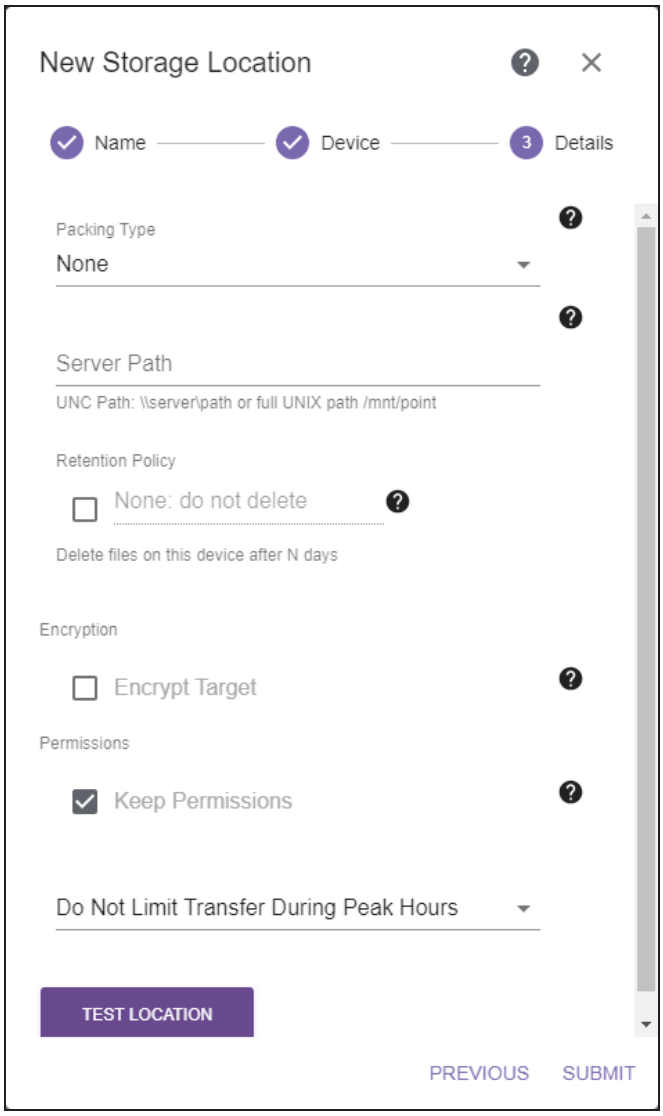


Figure 30 The New Storage Location Non-Spectra NAS Target Details dialog box.

3. Enter the file system **Server Path** to the NAS mount point (\\server\path or full UNIX path /mnt/point).

IMPORTANT

Storage location server paths should not overlap. For example:

- The storage location server path should not be a sub-directory of an existing storage location path.
- The storage location server path should not have as a sub-directory an existing storage location path.
- The storage location server path cannot be the same as an existing storage location path with different capitalization.

IMPORTANT The server path name should not be the same as a BlackPearl bucket that you plan to ingest. See Ingest Data in BlackPearl Bucket on page 123 for more information.

4. If you are configuring a target storage location, continue with Step 5. For a source storage location, configure the following:
   a. If desired, select **AD / LDAP Group** and enter an AD / LDAP group to restrict access to scan, migrate / store, and restore jobs, as well as file listings associated with the source, to members of the designated group and administrators. If you select this option and AD / LDAP is not configured or the entered user group does not exist, access is restricted to administrators. See Storage Location Security on page 84 for more information.
   b. If desired, select **Enable Versioning** to keep multiple versions of a file from the source storage location on the target storage location after multiple migrate / store jobs. See Versioning on page 83 for more information.
   c. If you selected **Enable Versioning**, select whether to create versions for **Changed Files Only**.
   d. If you selected **Enable Versioning**, select whether to limit the number of **Versions to Keep** and if so, enter or select the number to keep.
   e. Continue with Step 7 on page 107.
5. The following settings only apply to target storage locations.
   a. Select whether archived data should be packed into larger files for transfer, and which **Packing Type** to use. When migrating many small files, packing improves performance by reducing the total number of objects that are migrated and managed. This also reduces the total size of the database. Individual files in packs are tracked by StorCycle, and users may restore a single or multiple individual files which are stored in a pack. StorCycle packs can be accessed outside of the StorCycle solution using a tool to unzip or untar the packed file.

Notes:

- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files are added to packs until the pack reaches 10,000 files or reaches 10 GiB of data.

- Files are never split between packs.
- Up to five packs can be created at the same time.

b. If desired, select **Retention Policy** and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87 for more information.

Note: Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.

c. If desired, select **Encrypt Target** to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted. See Enable Encryption on page 210 for more information.

Note: Only users with a Crypto Officer role can enable or disable encryption.

Note: Only users with a Crypto Officer role can enable or disable encryption.

6. If desired, select **Keep Permissions** to preserve file permissions on the storage location.
7. Use the drop-down menu to select either:

- Do Not Limit Transfer During Peak Hours, below, or
- Limit Transfer During Peak Hours below

Do Not Limit Transfer During Peak Hours

If you selected **Do Not Limit Transfer During Peak Hours**, continue with Test and Submit the Storage Location on page 109.

Limit Transfer During Peak Hours

When you selected **Limit Transfer During Peak Hours**, the configuration options for limiting transfer display.

Note: Limiting transfer during peak hours only applies when reading from the storage location. If the Storage Location Type is Source, this occurs when the location is scanned or is the source of a migrate / store project. If the Storage Location Type is Target, this occurs when a restore is done of a file previously migrated / stored to the target.

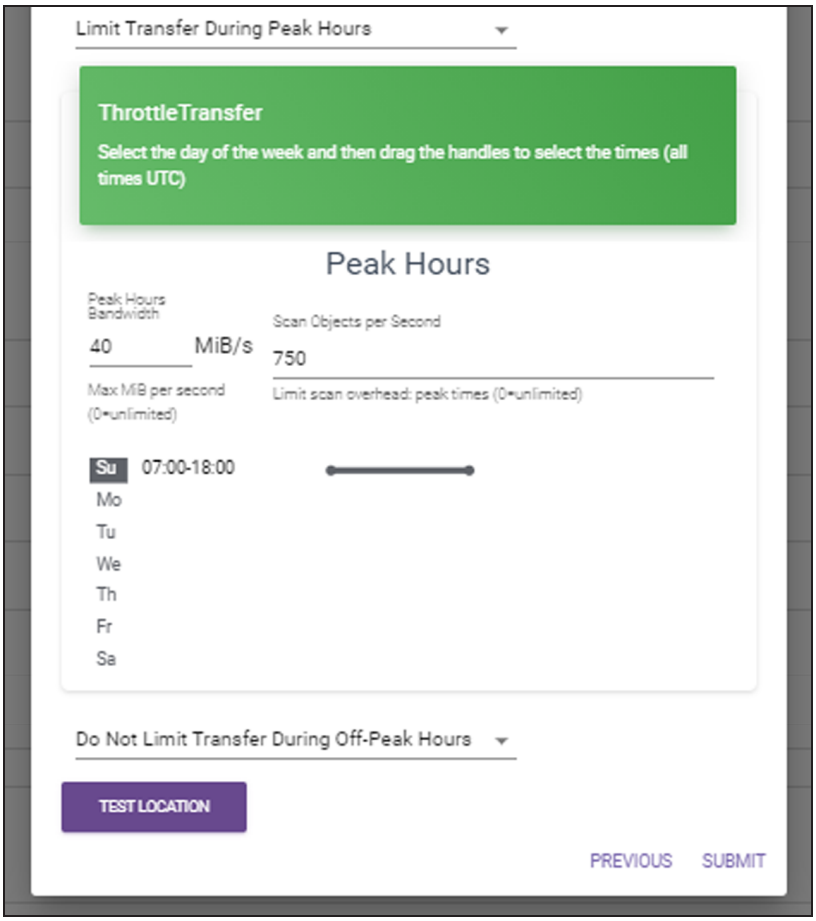


Figure 31 The Limit Transfer During Peak Hours configuration settings.

a. Enter the **Peak Hours Bandwidth**. The default is 40 MiB/s. Spectra Logic recommends starting with 10% of peak load and then adjust as necessary by editing the storage location.

b. Enter the maximum **Scan Objects per Second** during peak hours. The default is 750.

c. Select a day of the week for which you want to designate peak hours. The default peak hour selection of 07:00-18:00 (7:00 AM - 6:00 PM) displays. Select and move a handle to change the start and end times. Repeat this step for other days as necessary.

Note: The time range is in Coordinated Universal Time (UTC), not local time.

d. Use the drop-down menu to select either **Do Not Limit Transfer During Off-Peak Hours**, or **Limit Transfer During Off-Peak Hours**.

Do Not Limit Transfer During Off-Peak Hours

If you selected **Do Not Limit Transfer During Off-Peak Hours**, continue with Test and Submit the Storage Location on the next page.

Limit Transfer During Off-Peak Hours

When you selected **Limit Transfer During Off-Peak Hours**, the configuration options for limiting transfer display.

Note: Limiting transfer during off-peak hours only applies when reading from the storage location. If the Storage Location Type is Source, this occurs when the location is scanned or is the source of a migrate / store project. If the Storage Location Type is Target, this occurs when a restore is done of a file previously migrated / stored to the target.

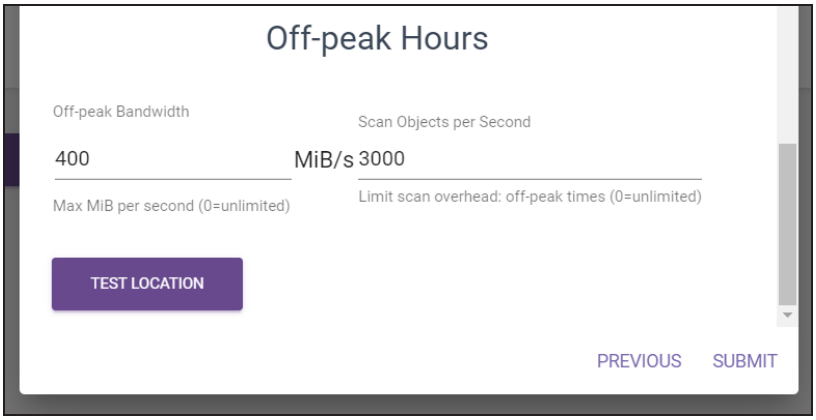


Figure 32 The Limit Transfer During Off-Peak Hours configuration settings.

i. Enter the **Off-Peak Bandwidth**. The default is 400 MiB/s. Spectra Logic recommends starting with 100% of peak load and then adjust as necessary by editing the storage location.

ii. Enter the maximum **Scan Objects per Second** during off-peak hours. The default is 3000.

Test and Submit the Storage Location

1. Click **Test Location** to verify that the server can connect to the storage location. If the StorCycle solution does not return a check mark indicating it can communicate with the storage location, you must resolve the error before submitting the location.
2. Click **Submit** to save the storage location.

Enter S3 Storage Location Information

Notes:
- Data on S3 source storage can only be migrated / stored to a BlackPearl storage location.
- Files migrated / stored from an S3 source to a BlackPearl storage location can only be restored to a Spectra or Non-Spectra NAS storage location.

If you select the **S3** storage type, the dialog box updates to display the following fields:

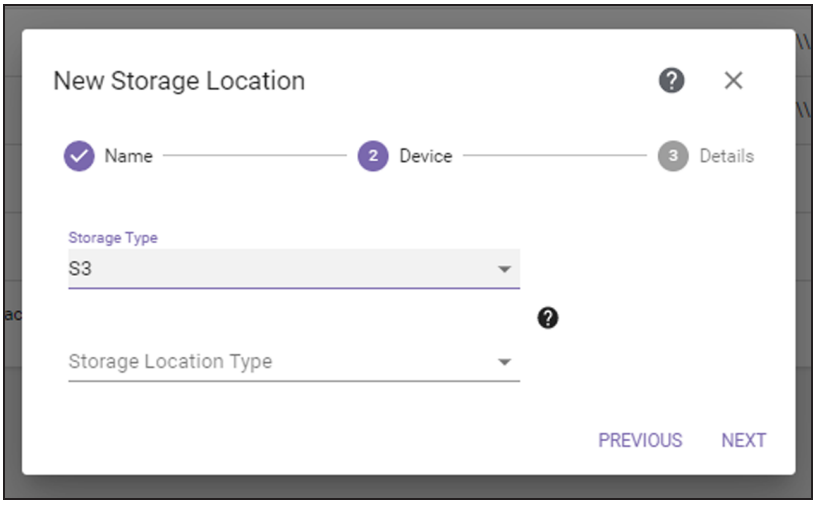


Figure 33 The New Storage Location S3 Device dialog box.

1. For **Storage Location Type**, select whether the storage location will act as a **Source** or a **Target**.
2. Click **Next**. The S3 Storage Location Details dialog box displays. The options that display are different if you are creating source or target storage. First you configure settings common to both types of storage, then use either the source or target storage instructions depending on the type of storage you are configuring.

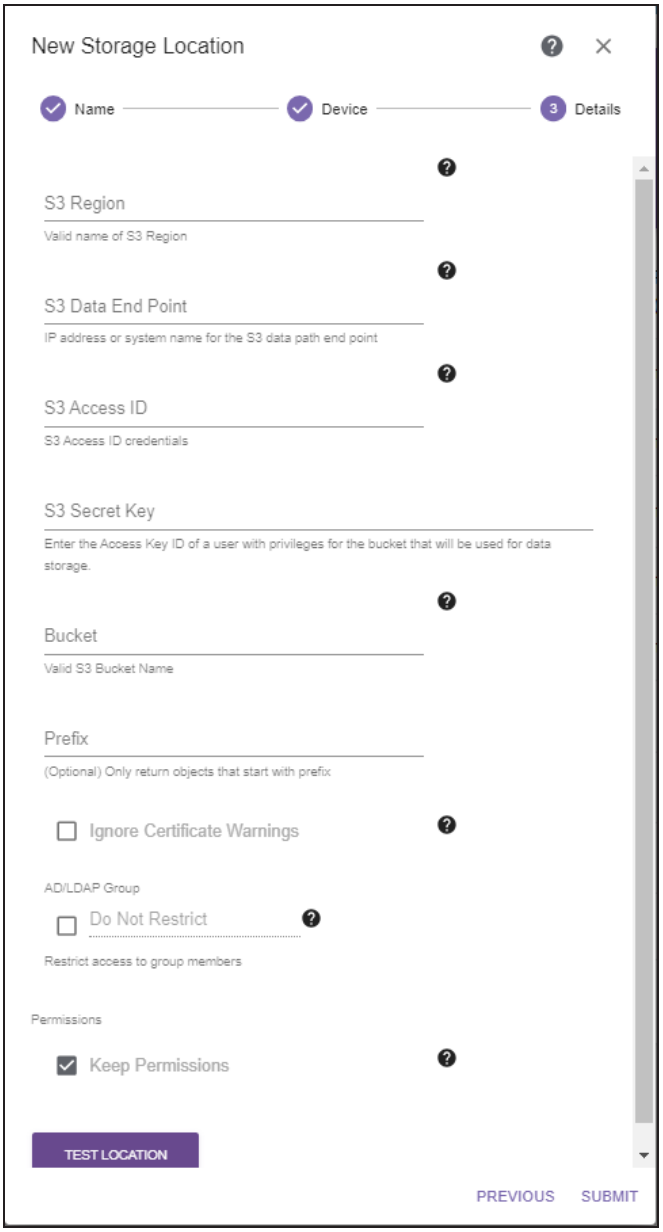


Figure 34 The New Storage Location S3 **Source** Details dialog box.

Figure 35 The New Storage Location S3 **Target** Details dialog box .

Steps for Both Storage Types

1. Enter an **S3 Region** or an **S3 Data End Point** in the format *xxx.xxx.xxx.xxx:port* (port is optional). For AWS specify **S3 Region** only. For non-AWS, specify and endpoint with HTTP or HTTPS.
2. Enter the **S3 Access ID** of a user with credentials for the S3 cloud and the bucket that will be used for data storage.
3. Enter the **S3 Secret Key** associated with the **S3 Access ID**.

4. Enter the name of the **Bucket** to be used for data storage.

CAUTION Make sure the target bucket is configured for versioning to avoid a migrate / store failing if a file with the same name already exists in the Bucket.

The bucket name must adhere to the Amazon S3 naming requirements. If the bucket does not exist, it is created.

S3 names have the following restrictions:

- Bucket names must comply with DNS naming conventions.
- Bucket names must be at least 3 and no more than 63 characters long.
- Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period (.).
- Bucket names can contain lowercase letters (a-z), numbers (0-9), and hyphens. You cannot use a hyphen at the beginning or end of a label.
- Bucket names cannot contain uppercase characters or underscores.
- Bucket names cannot be formatted as an IP address.

5. If desired, select **Ignore Certificate Warnings** to indicate that this is a trusted target and security certificate warnings should be ignored, even if it has a self-signed or missing security certificate.
6. Continue with either the **source storage** or **target storage** instructions below:
   - Steps for Source Storage below

     -OR-
   - Steps for Target Storage on the next page

Steps for Source Storage

1. If desired, enter a **Prefix**. Only objects that start with the prefix are considered for scans or migrate / store projects.
2. If desired, select **AD / LDAP Group** and enter an AD / LDAP group to restrict access to scan, migrate / store, and restore jobs, as well as file listings associated with the source, to members of the designated group and administrators. If you select this option and AD / LDAP is not configured or the entered user group does not exist, access is restricted to administrators. See Storage Location Security on page 84 for more information.
3. Continue with Final Steps for Both Storage Types on the next page.

Steps for Target Storage

1. Select whether archived data should be packed into larger files for transfer, and which **Packing Type** to use. When migrating many small files, packing improves performance by reducing the total number of objects that are migrated and managed. This also reduces the total size of the database. Individual files in packs are tracked by StorCycle, and users may restore a single or multiple individual files which are stored in a pack. StorCycle packs can be accessed outside of the StorCycle solution using a tool to unzip or untar the packed file.

Notes:
- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files are added to packs until the pack reaches 10,000 files or reaches 10 GiB of data.
- Files are never split between packs.
- Up to five packs can be created at the same time.

2. If desired, select **Retention Policy** and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87 for more information.

Note: Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.

3. If desired, select **Encrypt Target** to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted. See Enable Encryption on page 210 for more information.

Note: Only users with a Crypto Officer role can enable or disable encryption.

4. Continue with Final Steps for Both Storage Types below.

Final Steps for Both Storage Types

1. If desired, select **Keep Permissions** to preserve file permissions on the storage location.
2. Click **Test Location** to verify that the server can connect to the storage location. If the StorCycle solution does not return a check mark indicating it can communicate with the storage location, you must resolve the error before submitting the location. Error message display at the top of the create storage dialog box.
3. Click **Submit** to save the storage location.

Using AWS Glacier

Starting with StorCycle 4.0, Native Glacier storage locations are no longer supported. Native Glacier storage cannot be configured and any existing migrate / store jobs to Glacier fail. AWS Glacier is compatible with the StorCycle solution using AWS S3 bucket policies.

To use AWS Glacier Storage classes, create a zero-day policy on an AWS bucket. When the configured policy conditions are met, the policy immediately migrates the data to Glacier. Any policy configurations occur on the AWS bucket outside of the StorCycle solution.

IMPORTANT Starting with StorCycle 4.4 (estimated to release in 2025), you will not be able to restore any data previously migrated to Glacier using the StorCycle solution.

Enter Microsoft Azure Storage Location Information

Notes:
- To enter a Microsoft Azure Archive storage location, Enter Microsoft Azure Archive Storage Location Information on page 117.
- Microsoft Azure storage locations can only be target locations.

If you select the **MS Azure** storage type, the dialog box displays as shown:

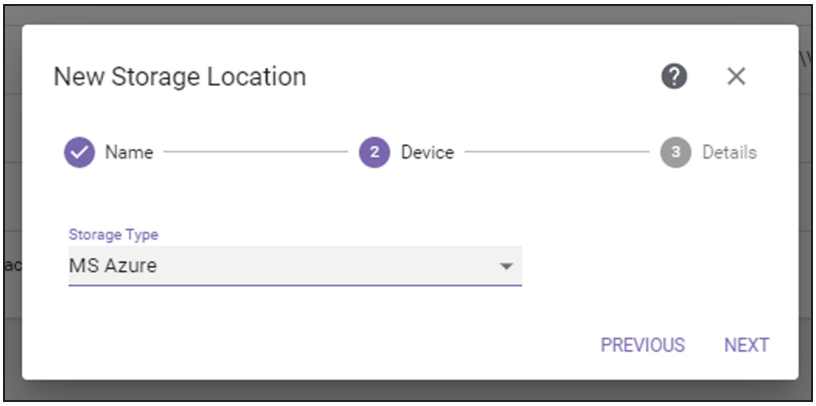


Figure 36 The New Storage Location MS Azure Device dialog box.

1. Click **Next**. The MS Azure Storage Location Details dialog box displays.

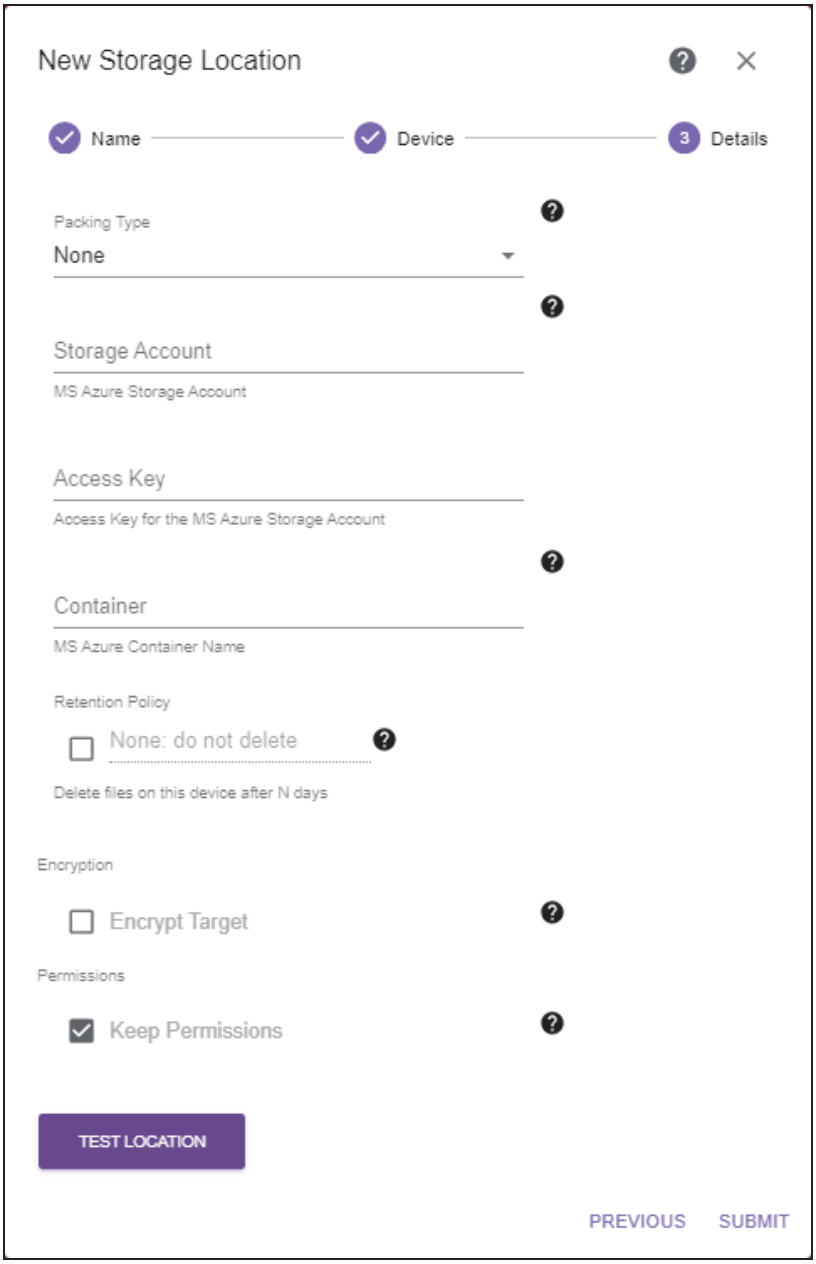


Figure 37 The New Storage Location MS Azure Details dialog box.

2. Select whether archived data should be packed into larger files for transfer, and, if so, which **Packing Type** to use.

   When migrating many small files, packing improves performance by reducing the total number of objects that are migrated and managed by the target system. Individual files in packs are tracked by StorCycle, and users may restore a single or multiple individual files which are stored in a pack.

   StorCycle packs can be accessed outside of the StorCycle solution using a tool to unzip or untar the packed file.

Notes:
- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files are added to packs until the pack reaches 10,000 files or reaches 10 GiB of data.
- Files are never split between packs.
- Up to five packs can be created at the same time.

3. Enter a Microsoft Azure **Storage Account** for the container to be used for data storage.
4. Enter the **Access Key** for the Storage Account.
5. Enter the name of the **Container** to be used for data storage.

CAUTION Make sure the storage account is configured for blob versioning to avoid migrate / store failures if a file with the same name already exists in the container.

The container name must adhere to the Microsoft Azure naming requirements. If the container does not exist, it is created.

Container names have the following restrictions:

- Container names must comply with DNS naming conventions.
- Container names may contain lower case letters, numbers and single dashes.
- Dashes must be preceded by and followed by letters or numbers.
- Bucket names must be at least 3 and no more than 63 characters long.

6. If desired, select the **Retention Policy** check box and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87 for more information.

Note: Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.

7. If desired, select the **Encrypt Target** check box to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted. See Enable Encryption on page 210 for more information.

Note: Only users with a Crypto Officer role can enable or disable encryption.

8. If desired, select **Keep Permissions** to preserve file permissions on the storage location.
9. Click **Test Location** to verify that the server can connect to the storage location. If the StorCycle solution does not return a check mark indicating it can communicate with the storage location, you must resolve the error before submitting the location.
10. Click **Submit** to save the storage location.

Enter Microsoft Azure Archive Storage Location Information

Notes:
- To enter a Microsoft Azure standard tier storage location, see Enter Microsoft Azure Storage Location Information on page 114.
- Microsoft Azure Archive storage locations can only be target locations.

If you select the **MS Azure Archive** storage type, the dialog box displays as shown:

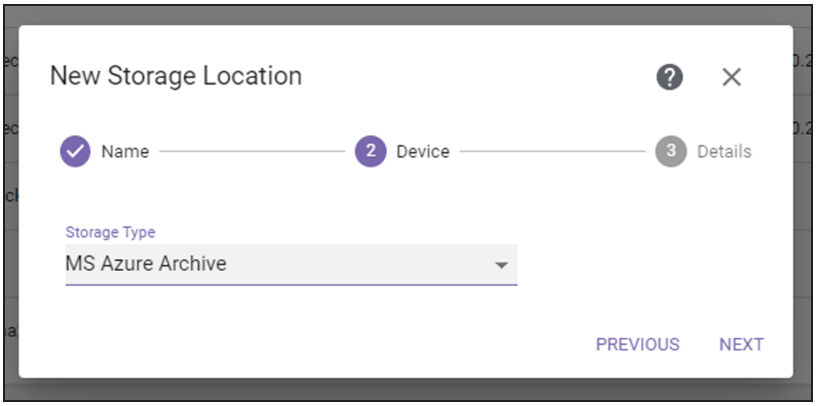


Figure 38 The New Storage Location MS Azure Archive Device dialog box.

1. Click **Next**. The MS Azure Storage Location Details dialog box displays.

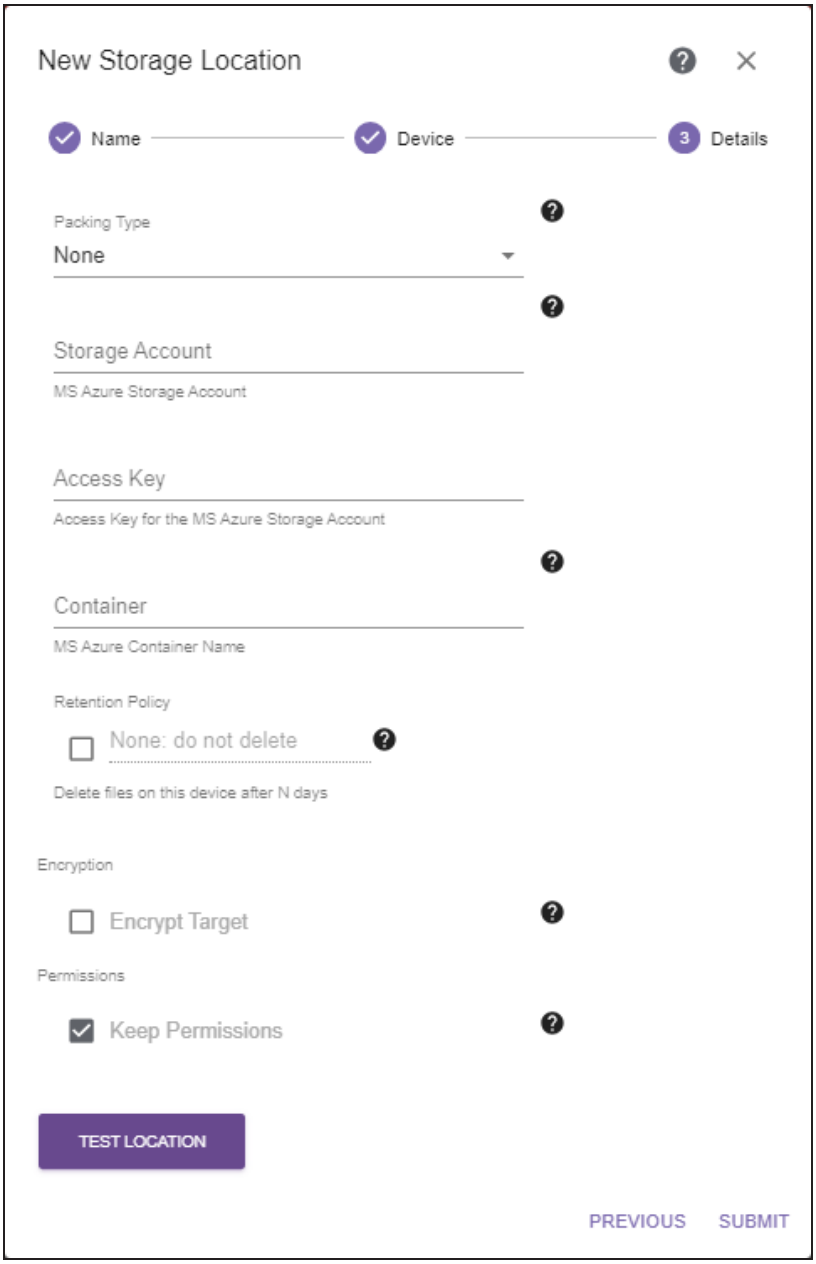


Figure 39 The New Storage Location MS Azure Archive Details dialog box.

2. Select whether archived data should be packed into larger files for transfer, and, if so, which **Packing Type** to use.

   When migrating many small files, packing improves performance by reducing the total number of objects that are migrated and managed by the target system. Individual files in packs are tracked by StorCycle, and users may restore a single or multiple individual files which are stored in a pack.

   StorCycle packs can be accessed outside of the StorCycle solution using a tool to unzip or untar the packed file.

Notes:
- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files are added to packs until the pack reaches 10,000 files or reaches 10 GiB of data.
- Files are never split between packs.
- Up to five packs can be created at the same time.

3. Enter a Microsoft Azure **Storage Account** for the container to be used for data storage.
4. Enter the **Access Key** for the Storage Account.
5. Enter the name of the **Container** to be used for data storage.

CAUTION Make sure the storage account is configured for blob versioning to avoid migrate / store failures if a file with the same name already exists in the container.

The container name must adhere to the Microsoft Azure naming requirements. If the container does not exist, it is created.

Container names have the following restrictions:

- Container names must comply with DNS naming conventions.
- Container names may contain lower case letters, numbers and single dashes.
- Dashes must be preceded by and followed by letters or numbers.
- Bucket names must be at least 3 and no more than 63 characters long.

6. If desired, select the **Retention Policy** check box and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87 for more information.

Note: Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.

7. If desired, select the **Encrypt Target** check box to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted. See Enable Encryption on page 210 for more information.

Note: Only users with a Crypto Officer role can enable or disable encryption.

8. If desired, select **Keep Permissions** to preserve file permissions on the storage location.
9. Click **Test Location** to verify that the server can connect to the storage location. If the StorCycle solution does not return a check mark indicating it can communicate with the storage location, you must resolve the error before submitting the location.
10. Click **Submit** to save the storage location.

CLONE A BLACKPEARL STORAGE LOCATION

To clone a BlackPearl storage location, select the **Actions** menu and select **Clone** next to the BlackPearl storage location on the Storage screen (see Figure 17 on page 90). The *BlackPearl name* Clone dialog box displays.

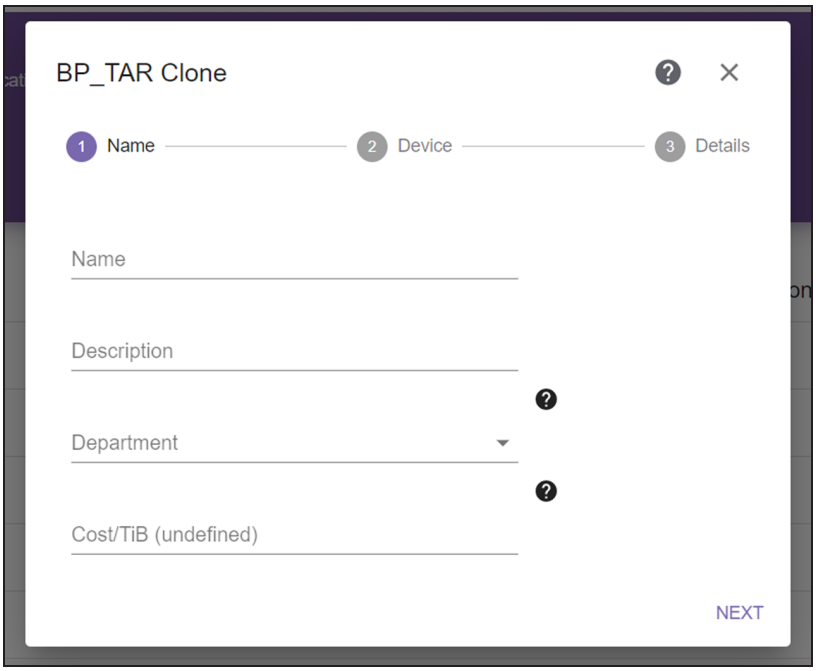


Figure 40 The *BlackPearl name* Clone Name dialog box.

1. Enter a unique **Name** for the storage location.
2. If desired, enter a **Description** for the storage location.
3. If desired, use the drop-down list to select the **Department** responsible for the storage location costs. To create a department, see Configure Departments on page 220.
4. If desired, enter the **Cost/TiB** to use for storage location costs.

Note: See Configure Global Settings on page 135 to change the currency.

5. Click **Next**. The *BlackPearl name* Clone Device dialog box displays.

Note: The information on this screen cannot be changed.

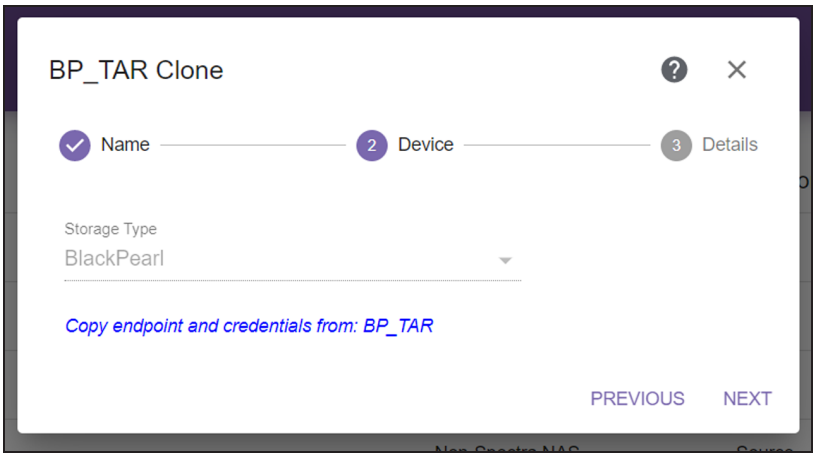


Figure 41 The *BlackPearl name* Clone Device dialog box.

6. Click **Next**. The *BlackPearl name* Clone Details dialog box displays.

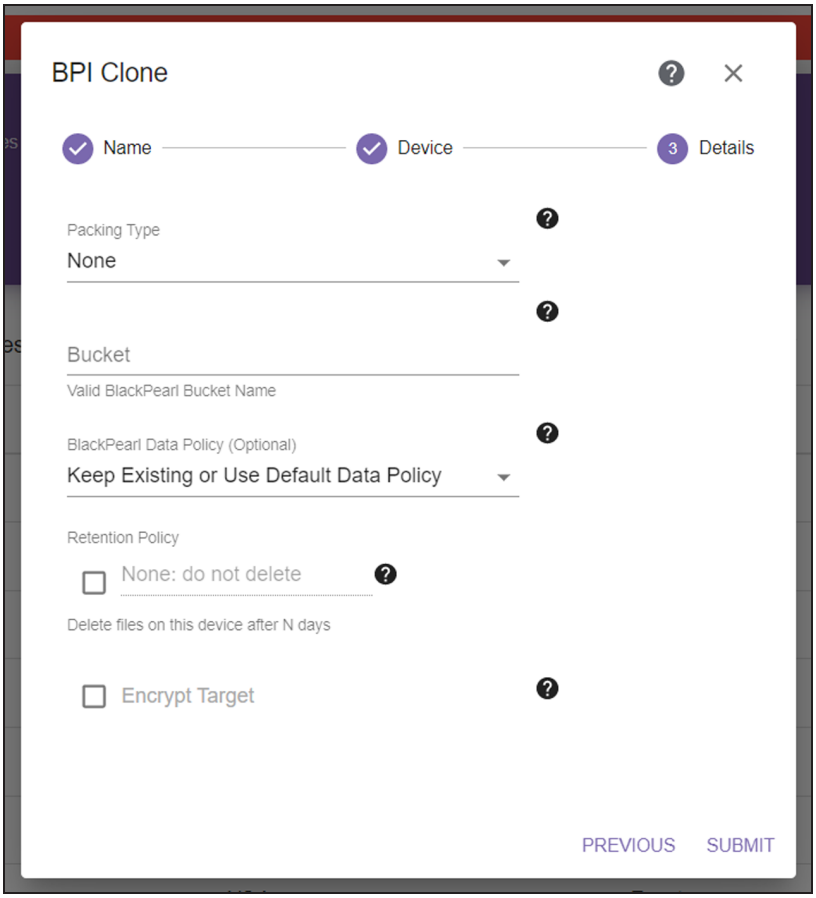


Figure 42 The *BlackPearl name* Clone Details dialog box (target shown).

7. Select whether archived data should be packed into larger files for transfer, and, if so, which **Packing Type** to use. Packing reduces the number of objects sent to a BlackPearl system and larger files transfer to a BlackPearl system faster than multiple smaller files.

Notes:
- Spectra Logic recommends using packing when a majority of files are smaller than 5 MiB and no files are larger than 10 GiB.
- Spectra Logic recommends using **ZIP** for Windows clients and **TAR** for UNIX clients.
- Files continue to be added to packs until the pack reaches 10,000 files or goes beyond 10 GiB of data.
- Files are never split between packs.
- Up to five packs can be created at the same time.

8. Enter the name of the **Bucket** to be used for data storage. If the bucket does not exist, it is created.

CAUTION Make sure the target bucket uses a data policy with versioning enabled to avoid migrate / store jobs failing if a file with the same name already exists in the bucket.

Note: Bucket names must meet the following criteria:
- Bucket names must be at least 1 character long and not more than 63 characters long.
- Bucket names must not contain special characters such as @, $, #, %, {, }, or |.

9. If the bucket already exists, you can select **Keep Existing or Use Default Data Policy** or **View Existing Bucket Policy** to see the data policy assigned to the bucket.

   If the bucket is new, you can select **Keep Existing or Use Default Data Policy** or a listed data policy.

10. If desired, select the **Retention Policy** check box and enter or select the desired number of days to retain files on this storage location before the StorCycle solution automatically deletes the files for compliance or capacity recovery. Clear the **Retention Policy** check box to keep files permanently. See Retention Policy Best Practices on page 87.

Note: Retention policies are only supported for data center and enterprise licenses. See Licensing on page 42 for more information.

11. If desired, select the **Encrypt Target** check box to encrypt data sent to this target location. Clear the **Encrypt Target** check box if you do not want data sent to the target encrypted. See Enable Encryption on page 210 for more information.

Note: Only users with a Crypto Officer role can enable or disable encryption.

12. Click **Submit** to save the storage location.

INGEST DATA IN BLACKPEARL BUCKET

A bucket on a BlackPearl system with data added outside of the StorCycle solution can be ingested so that the objects in the bucket are managed by the StorCycle solution, allowing you to restore the contents of the bucket.

Notes:
- You cannot ingest a bucket previously used as a target for a migrate / store project.
- A second ingest of the same storage location will ingest new files added to the bucket outside of the StorCycle solution, and will update files changed in the BlackPearl bucket.
- If the ingested bucket name matches a StorCycle server path, and the storage location and bucket contain file(s) with the same name(s), the ingest of those files will fail.

1. To ingest a BlackPearl bucket, first configure it as a BlackPearl storage location. See Configuring Storage on page 89.

Note: You cannot ingest a storage location configured to use encryption or packing.

2. On the storage screen (see Figure 17 on page 90), select the **Actions** menu and select **Ingest** next to the BlackPearl storage location. The *BlackPearl name* Ingest dialog box displays.

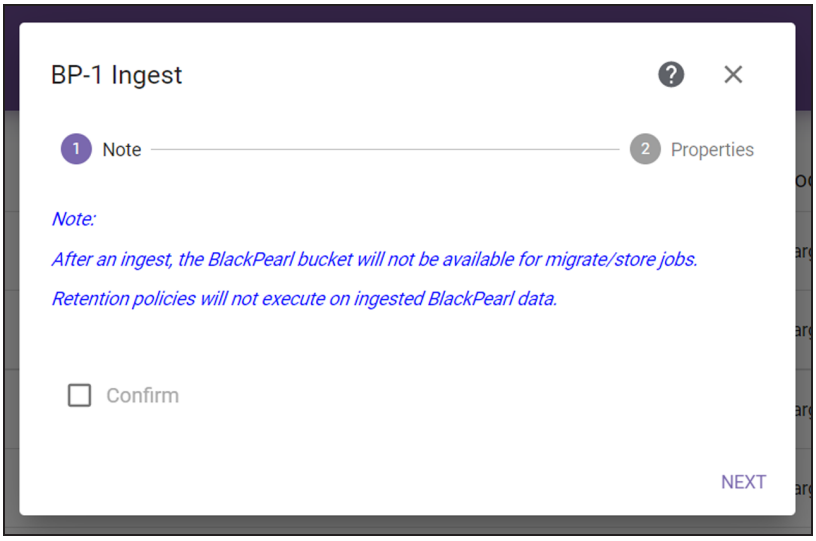


Figure 43 The *BlackPearl name* Ingest Note dialog box.

3. Select the check box to **Confirm** that you understand that the BlackPearl bucket is not available for migrate / store jobs after the ingest, and that retention policies do not delete ingested data.

4. Click **Next**. The *BlackPearl name* Ingest Properties dialog box displays.

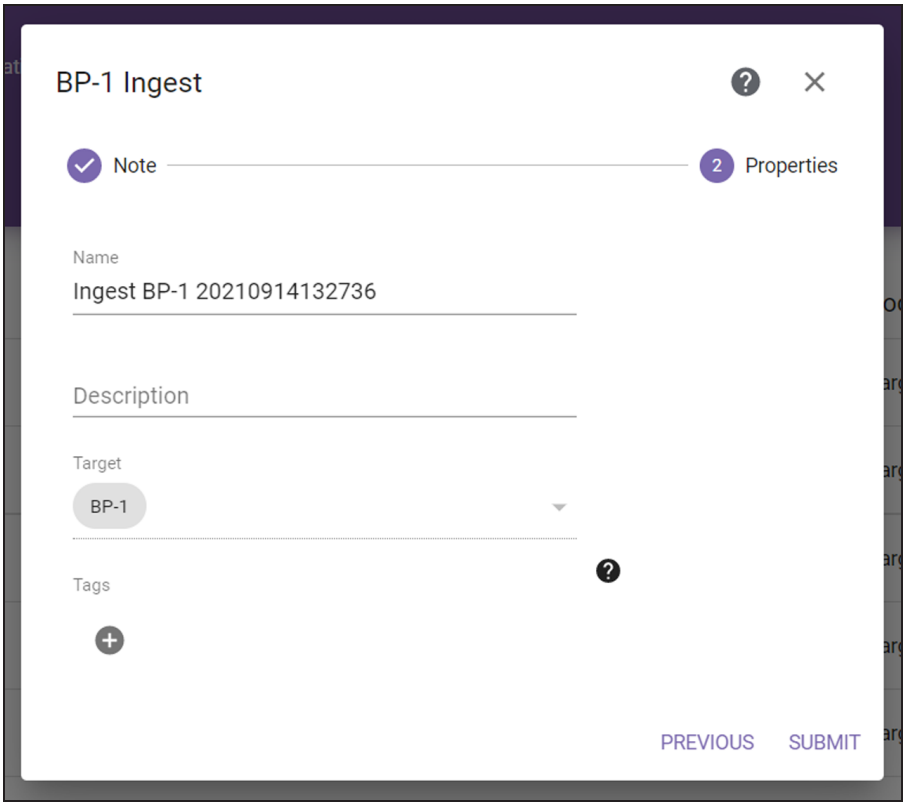


Figure 44 The *BlackPearl name* Ingest Properties dialog box.

5. If desired, edit the **Name** for the ingest job.
6. If desired, enter a **Description** for the ingest job.
7. If desired, under **Tags**, click the plus (+) sign to add a new line for entering tags to apply to this task for searching purposes. Search by Tag allows you to search for any sub string within the tag. See Search by Tag on page 197 for more information.
8. Click **Submit** to ingest the data.

Edit a Storage Location

To edit a storage location, select the **Actions** menu and select **Edit** next to the storage location that you want to edit (see Figure 17 on page 90).

Any field in a storage location configuration can be edited until it has been used in a project. See Configuring Storage on page 89 for field descriptions.

Once a storage location has been used in a project, some fields are no longer editable. Those fields are grayed out.

Only a user with a Crypto Officer role can enable or disable encryption.

Retire/Delete a Storage Location

Starting with the StorCycle 4.3.0 solution, you can retire or delete storage locations. Retired storage locations can also be reinstated.

Note: To delete storage locations in earlier versions of the StorCycle solution, contact Spectra Logic Technical Support (see Contacting Support).

Retire a Storage Location

Retiring a storage location disables the location so that it cannot be used in any future projects, but the data archived to the storage location can still be searched and restored to other locations using the StorCycle solution.

After the storage location is retired, it can be reinstated to allow the location to be used again for migrate / store projects.

Use the instructions in this section to retire a storage location.

1. Using the **Actions** drop-down menu, select Retire. The Retire / Delete window displays.
2. Using the **Delete Type** drop-down menu, select **Retire Location**.
3. Click **Submit**.

Reinstate a Storage Location

You can reinstate a retired storage location to allow it to resume normal operations and make it available for migrate / store projects again.

1. Use the instructions in this section to reinstate a storage location.
2. Using the **Actions** drop-down menu, select **Reinstate**. The Reinstate window displays.
3. Click **Submit**.

Delete a Storage Location

Deleting a location removes the location from the StorCycle environment and deletes all objects associated with the storage location from the application database. Data is not deleted from target media, but the objects cannot be restored using the StorCycle solution.

Deleting a storage location **cannot** be undone, but the storage can be recreated at a later date using the New Storage Location wizard.

IMPORTANT Using the user interface to delete a storage location only deletes it from the StorCycle environment. Data on target media **is not deleted**.

CAUTION Using API commands to delete a storage location deletes it from the StorCycle environment. The API command may **optionally delete all data** on the storage target. Spectra Logic recommends contacting Spectra Logic Technical Support before using the API parameter to delete all data.

Use the instructions in this section to delete a storage location.

1. Using the **Actions** drop-down menu, select Retire. The Retire / Delete window displays.
2. Using the **Delete Type** drop-down menu, select **Delete Location**. The delete confirmation box displays.
3. Enter `DELETE LOCATION` in the confirmation box.
4. Click **Submit**.

Note: Depending on the number of files, it may take several minutes for the storage to complete the deletion process. Spectra Logic recommends allocating approximately 1 minute for every 15,000 objects.

Chapter 6 - Required Settings

This section provides instructions for configuring settings required by the StorCycle solution. You must have storage configured on the StorCycle solution before following the steps in this chapter. See Storage on page 81 for information on creating storage.

DATABASE BACKUP

The StorCycle solution requires daily database backups configured and scheduled before any migrate / store jobs can run.

IMPORTANT If something happens to the StorCycle database and you do not have a backup, you will lose information about what files are migrated and where they are located.

IMPORTANT Database backups are specific to each operating system. Database backups and the Database Archive and Restore actions cannot be used to migrate the database across operating system server platforms. For example, you cannot restore a database to a Windows system if it was originally created by a Linux system, and vice versa.

The Jobs pane of the main dashboard (see Figure 114 on page 228) provides the date and time for the last successful Database Backup. The background color for the Database Backup status indicates the age of the last successful backup:

- **White** — Less than one day old.
- **Yellow** — One to seven days old.
- **Red** — Greater than seven days old.

Note: The StorCycle solution displays a red banner message on the user interface to remind administrators if a daily database did not run in the last 24 hours.

Post Archive Action Delay

The StorCycle solution requires additional database protection for any migrate / store job that removes or replaces original source files. The StorCycle solution requires the completion of two successful database backups before the removal or replacement occurs.

Creating a Database Backup

Use the instructions below to configure a database backup.

Note: It is recommended to check the backup directory after creating your first database backup to verify the backup completed as expected.

1. Click **Settings** in the toolbar and then select **Database Backup**. The Database Backup screen displays showing recurring and single run Database Backup Projects and database backup jobs.

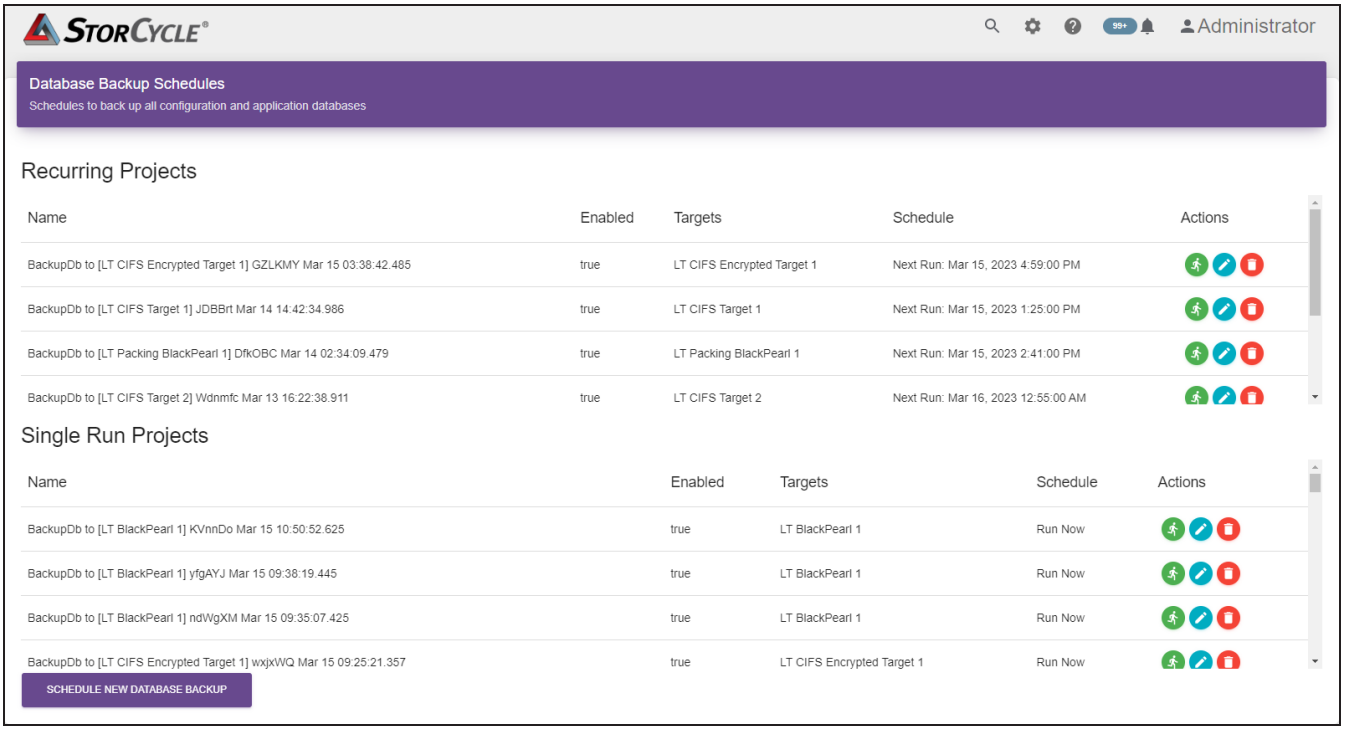


Figure 45 The Database Backup screen.

2. Click **Schedule New Database Backup**.

Schedule a New Database Backup—Database Backup Project Name

IMPORTANT Spectra Logic recommends that you schedule daily database backups.

The Schedule New Database Backup dialog box displays.

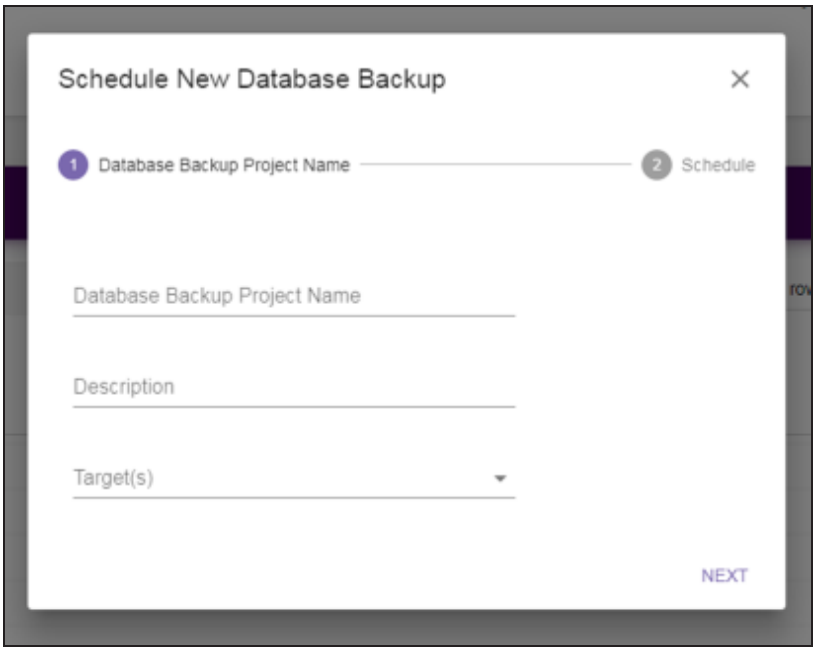


Figure 46 The Schedule New Database Backup dialog box.

1. Enter a unique name in the **Database Backup Project Name** field.

IMPORTANT A project name must be unique across all scan, migrate / store, restore, and database backup projects. Names of deleted projects cannot be reused.

2. If desired, enter a **Description** for the database backup project.
3. From the **Target(s)** drop-down, select one to three previously configured storage location. See Storage on page 81 for instructions for configuring a storage location. Spectra Logic strongly recommends selecting two targets which are stored in geographic locations separate from the StorCycle server.
4. Click **Next** to continue.

Schedule a New Database Backup—Schedule

The Schedule screen of the Database Backup wizard displays.

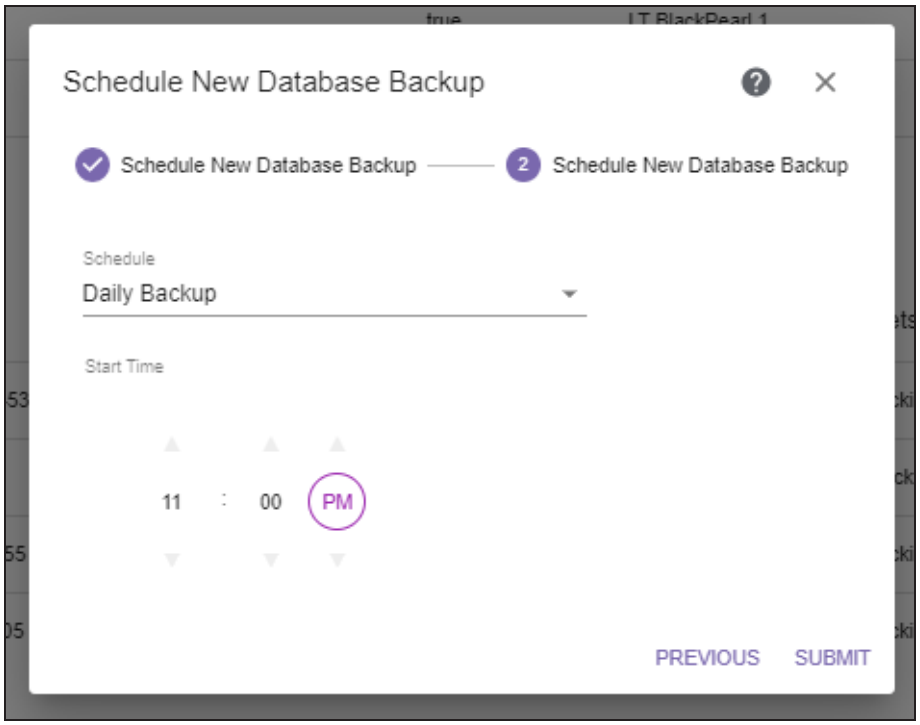


Figure 47 The Schedule screen of the Database Backup wizard.

Using the **Schedule** drop-down menu, select to **Backup Now**, **Set Recurring Schedule**, or **Set Backup Time**. The dialog box updates to show the configuration fields required for the selected schedule type. Continue with the applicable section below:

- Set Daily Backup on the next page
- Backup Now on the next page
- Backup Now on the next page

Set Daily Backup

If **Daily Backup** is selected, the dialog box displays the following fields:

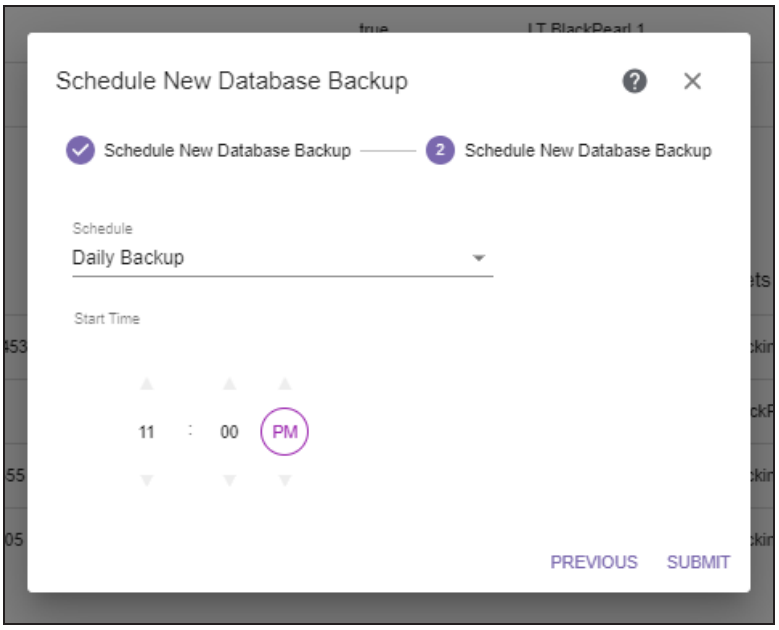


Figure 48 Setting a recurring schedule.

1. Use the up and down arrows to select the **Start Time** for the backup project. The default is 11:00 PM local machine time.
2. Click **Submit** to save the backup project. The job runs at the scheduled time.

Backup Now

If you selected **Backup Now**, click **Submit**. The backup job runs immediately.

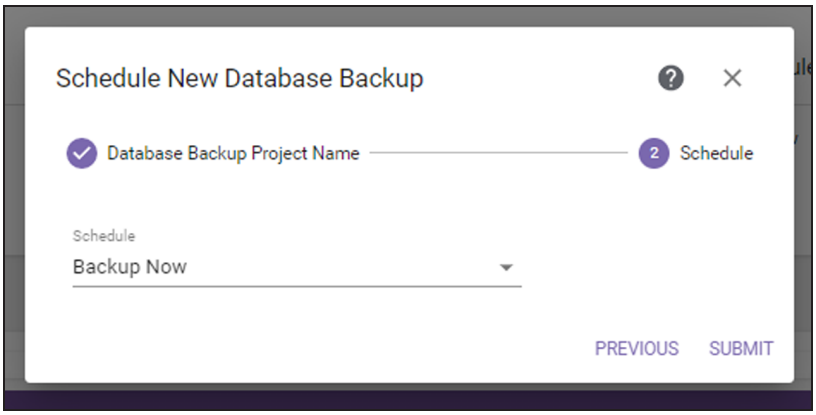


Figure 49 Select Backup Now.

Set Backup Time

If you select **Set Backup Time**, the dialog box updates to display the following fields:

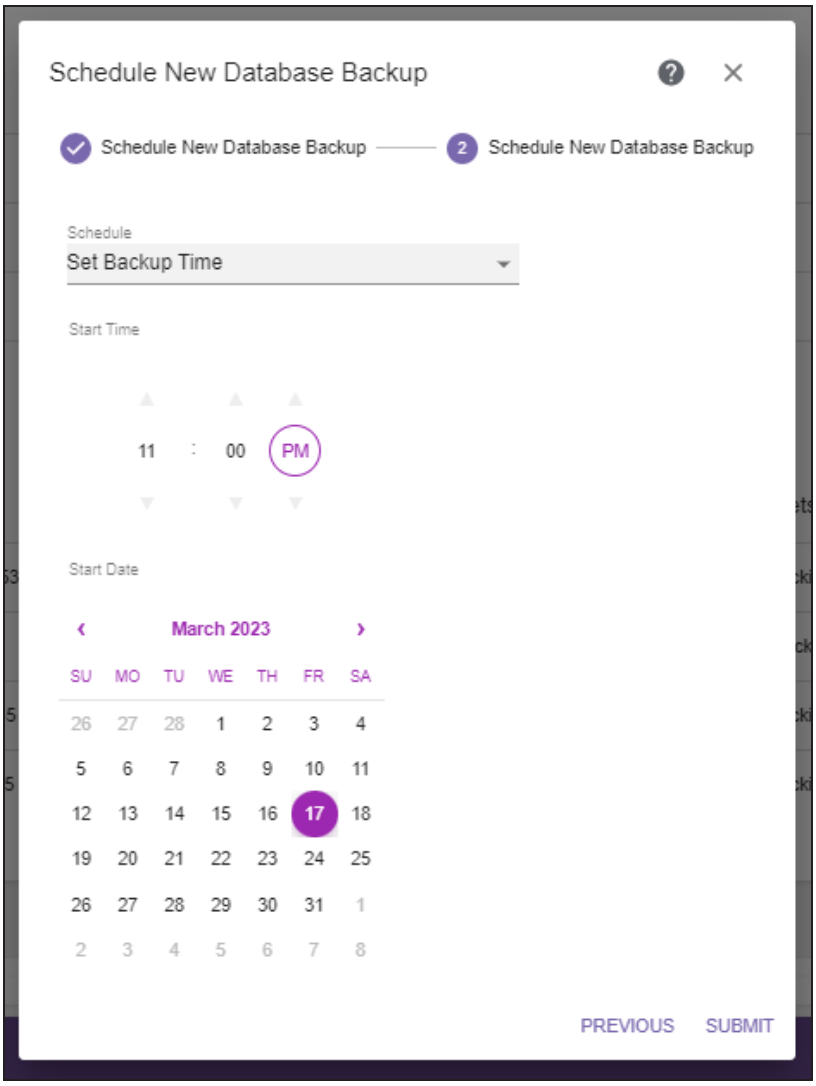


Figure 50 Setting a start time.

1. Use the up and down arrows to select the **Start Time** for executing the backup project. The default is 11:00 PM local machine time.
2. Using the calendar, select the **Start Date** on which to execute the database backup. The default is the current date.
3. Click **Submit** to save the backup project. The job runs as scheduled.

Run a Database Backup Project

To run a recurring or single-run Database Backup project, **Run** next to the project on the Database Backup screen (see Figure 45 on page 129). The Database Backup job runs immediately.

Cancel a Database Backup Job

To cancel a queued, verifying, or active database backup job, click **Cancel** next to the job on the Database Backup screen (see Figure 45 on page 129), or the Active and Completed Jobs screen (see Figure 116 on page 230). A confirmation screen displays. Click **Cancel Job** to confirm the cancellation.

Canceling a Database Backup job does not stop recurring Database Backup projects from running again. To stop a project with a recurring schedule from running again, see Disable a Database Backup Project.

Edit a Database Backup Project

To edit a database backup project, click **Edit** next to the project on the Database Backup screen. When editing the database backup project, you can change the Description, Target(s), and Schedule for the backup project. The name cannot be changed.

Disable a Database Backup Project

Disabling a Database Backup project stops projects with recurring schedules from running again and removes it from the list of projects on the Database Backup screen (see Figure 45 on page 129).

To disable a Database Backup project, click **Disable** next to the project on the Database Backup screen (see Figure 45 on page 129). A confirmation screen displays. Click **Delete** to confirm disabling the project.

Note: Even after disabling the project, the project name cannot be reused.

CONFIGURE GLOBAL SETTINGS

If desired, use the instructions below to edit the Global Settings.

1. Click **Settings** in the toolbar and then select **Configuration > Global Settings**. The Global Settings screen displays showing the current global settings.

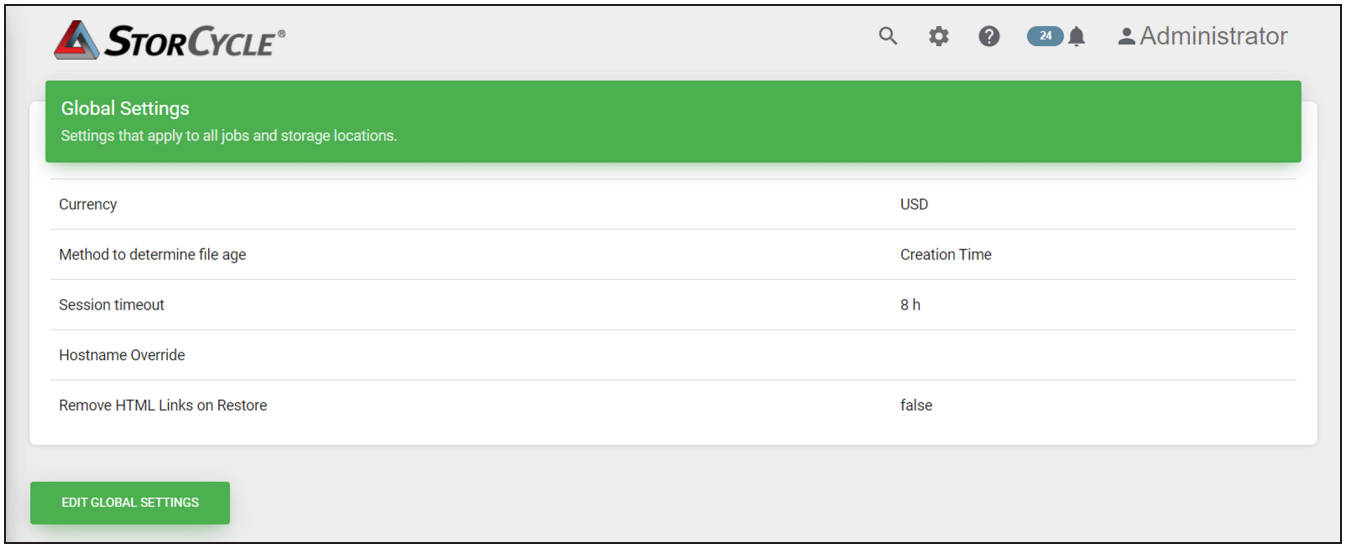


Figure 51 The Global Settings screen.

2. Click **Edit Global Settings**. The Global Settings dialog box displays.

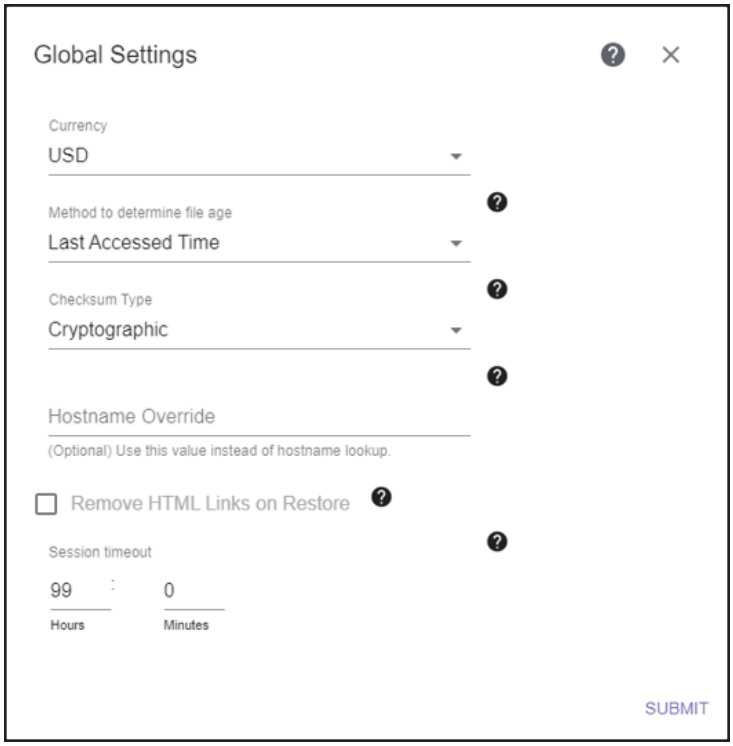


Figure 52 The Global Settings dialog box.

3. Select the currency to use when tracking costs. The default is USD.

Note: No conversion of previously entered values is done when the currency is changed. Only the currency symbol changes.

- **AUD**—Australian dollar
- **CAD**—Canadian dollar
- **CHF**—Swiss franc
- **EUR**—Euro
- **GBP**—British pound sterling
- **INR**—Indian rupee
- **KRW**—South Korean won
- **MXN**—Mexican peso
- **NZD**—New Zealand dollar
- **USD**—United States dollar
- **YEN**—Japanese yen

4. Select the **Method to determine file age**:

Note: Changing this setting only affects future scans. You must rescan storage locations after making the change to update values in the database.

- **Last Access Time**—The date and time the file was last read or written. This is the default and recommended method to use to prevent moving files that are being used.
- **Creation Time**—The date and time the file was initially created.
- **Last Modified Time**—The date and time the file was last written.

5. Select the **Checksum Type** to use for calculating checksums on files during a scan, migrate, or restore. The Default option uses XXH64 checksums. Cryptographic option uses B2B-256 checksums.

6. If desired, enter a URL for a **Hostname Override** to use instead of a hostname lookup in HTML links created to replace migrated / stored files.

Note: You must restart the StorCycle service before a new **Hostname Override** becomes active. See Start, Stop, and Restart the Services on page 70.

7. Select whether HTML links should be removed when files are restored to the same directory from which a migrate / store with the option to replace files with HTML links was done.

8. In the **Session Timeout** field, use the arrows to enter how long the current login to the Spectra StorCycle user interface can remain active. The default is eight hours and the maximum is 99 hours.

Note: Changing the session timeout value does not extend the current session. The new session timeout setting takes effect the next time you login.

9. Click **Submit** to save the Global Settings.

CONFIGURE ACTIVE DIRECTORY / LDAP

Notes:
- The StorCycle solution uses the domains configured on the server, including multiple domains, to access a DNS (Domain Name System) to resolve UNC (Universal Naming Convention) paths over the domain and uses Active Directory / LDAP to verify restore users are valid on the domain.
- StorCycle does not support anonymous requests to Active Directory / LDAP. In order to receive e-mail updates, users must have valid Active Directory / LDAP credentials.

If desired, use the instructions below to configure Active Directory / LDAP.

1. Click **Settings** in the toolbar and then select **Configuration > Active Directory / LDAP**. The Active Directory / LDAP Settings screen displays showing the current Active Directory / LDAP settings.

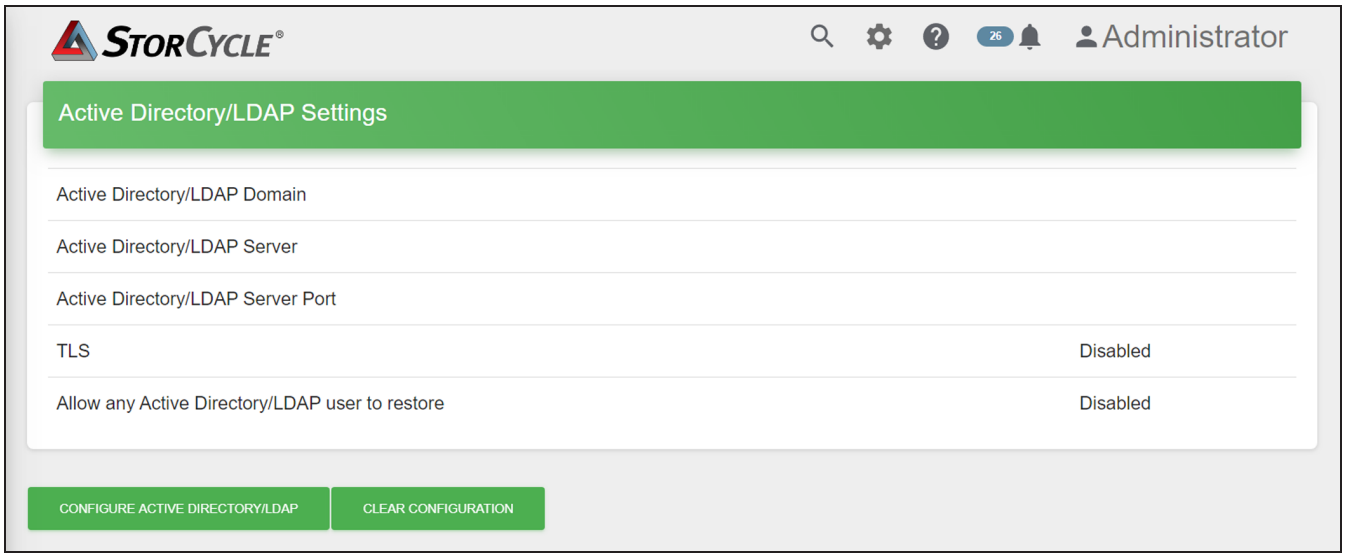


Figure 53 The Active Directory / LDAP Settings screen.

2. Click **Configure Active Directory / LDAP**. The Active Directory / LDAP Settings dialog box displays.

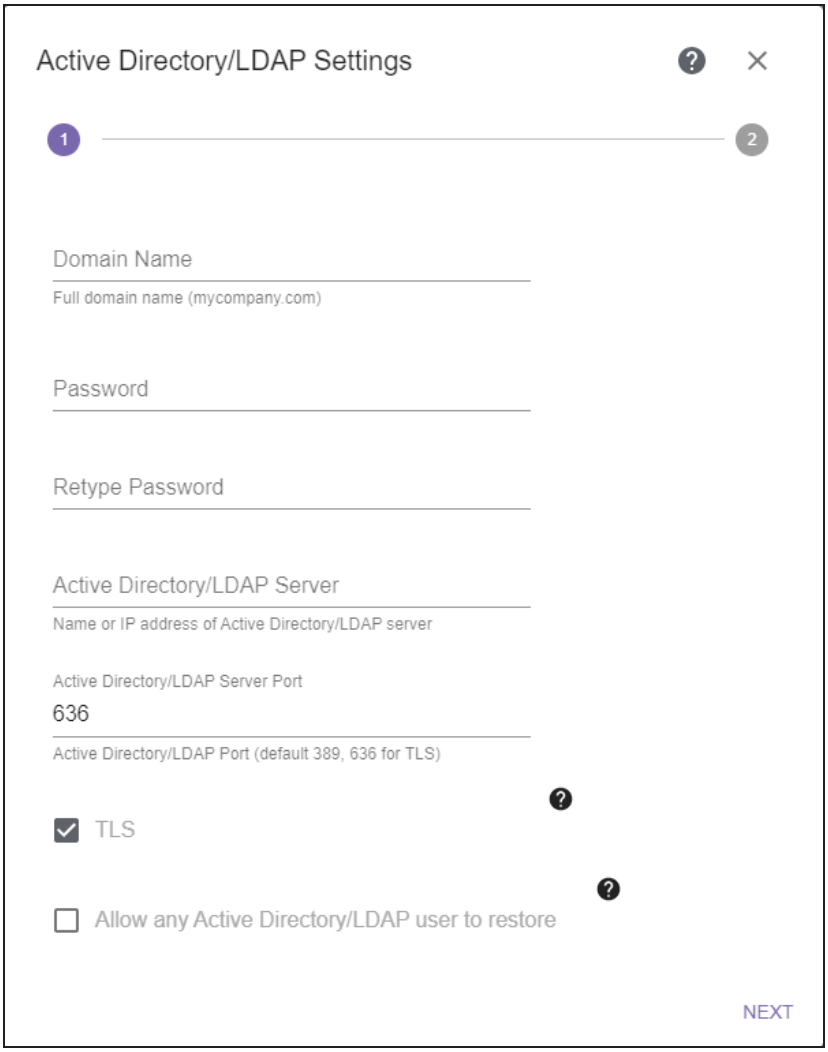


Figure 54 The Active Directory / LDAP Settings dialog box screen 1.

3. Enter the Active Directory **Domain Name** in the format *Domain*.com.
4. Enter and retype the **Password** for a user authorized to make Active Directory / LDAP queries.
5. Enter the IP address or hostname for the **Active Directory / LDAP Server**.
6. If desired, modify the **Active Directory / LDAP Server Port** to connect to the Active Directory server.
7. Select or clear the **TLS** check box. If selected, the StorCycle solution uses secure SSL/TLS to connect to the server. Spectra Logic recommends enabling SSL/TLS. The StorCycle solution supports TLS 1.0, 1.1, and 1.2.
8. Select or clear **Allow any Active Directory / LDAP user to restore**. If selected, any Active Directory / LDAP user on the domain can restore files even if they are not configured as a StorCycle user. These users can only restore files using an HTML link.

Note: Restore only Active Directory / LDAP users count against the licensed user limit.

9. If you selected **Allow any Active Directory / LDAP user to restore**, select whether to **Limit Daily Restores** to limit the amount of data an AD / LDAP user can restore each day and if selected, enter the **Daily Restore Limit**. The daily limit is from midnight to midnight UTC.

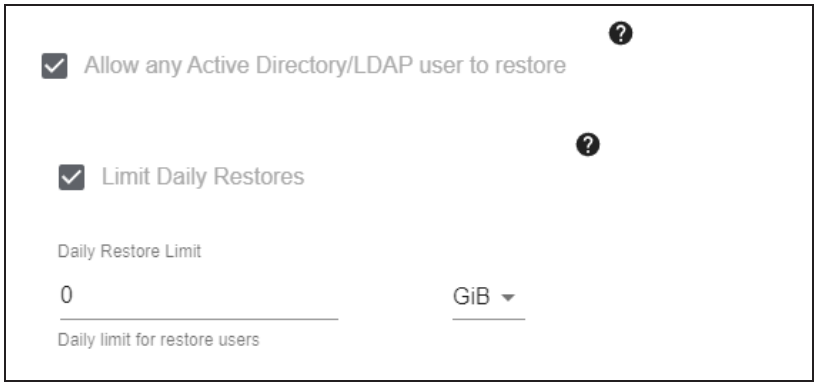


Figure 55 The Active Directory / LDAP Settings dialog box with **Allow any Active Directory / LDAP user to restore** selected.

10. Click **Next**. The second screen of the Active Directory / LDAP Settings dialog displays.

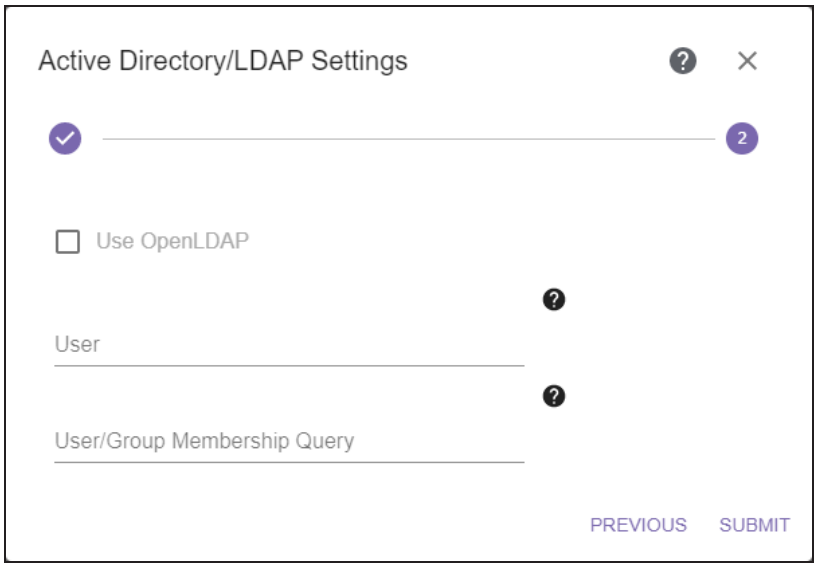


Figure 56 The Active Directory / LDAP Settings dialog box screen 2 without **Use OpenLDAP** selected.

11. Select whether or not to **Use OpenLDAP**. If you select **Use OpenLDAP**, continue with Configure Active Directory / LDAP Using OpenLDAP on the next page. If you do not select to use OpenLDAP, continue to Step 12 on page 139.

12. Enter a **User**, in the format user@domain, for the user associated with the passwords on the previous screen. The user must be authorized to make Active Directory / LDAP queries.

13. If desired, enter a custom **User / Group Membership Query**.

IMPORTANT Only system administrators who have an understanding of the organizations domain settings should modify the AD/LDAP group search query.

14. Click **Submit** to save the Active Directory / LDAP settings.

Configure Active Directory / LDAP Using OpenLDAP

If you selected **Use OpenLDAP**, the dialog box updates to display the OpenLDAP setting fields.

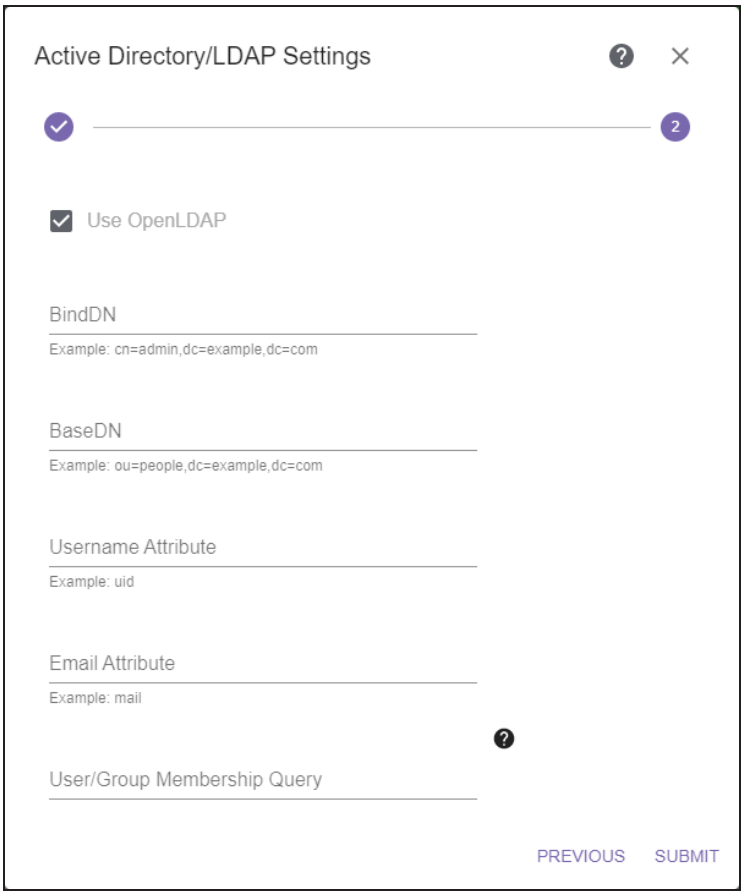


Figure 57 The Active Directory / LDAP Settings dialog box with **Use OpenLDAP** selected.

1. Enter the **BindDN**, for example `cn=admin, dc=example, dc=com`. This is the credential used to authenticate to the LDAP server and perform operations.
2. Enter the **BaseDN**, for example `cn=people, dc=example, dc=com`. This specifies the root location for the LDAP search for user accounts.
3. Enter the **Username Attribute**, for example a UID, for the user associated with the passwords on the previous screen. The user must be authorized to make Active Directory / LDAP queries.

4. Enter the **Email Attribute**, for example `mail`.
5. If desired, enter a custom **User/Group Membership Query**.

IMPORTANT Only system administrators who have an understanding of the organizations domain settings should modify the AD/LDAP group search query.

6. Click **Submit** to save the Active Directory / LDAP settings.

CONFIGURE USERS

Configure users to manage access to the server. The number of users may be restricted by the license installed. See Licensing on page 42 for more information.

The table below lists the type of **User Roles**.

User Role	Description
Administrator	Administrators can access the StorCycle user interface, migrate and restore data, and change the configuration settings, except encryption.
Storage Manager	Storage Managers can view the StorCycle console and migrate and restore data, but cannot change the configuration. **Note:** This is the default user role.
Crypto Officer	A Crypto Officer has all Administrator permissions, and can also configure encryption. **Note:** Only a Crypto Officer can configure another Crypto Officer.

Use the instructions below to configure a new user.

1. Click **Settings** in the toolbar and then select **Configuration > Users**. The Users screen displays showing all users currently configured in the software.

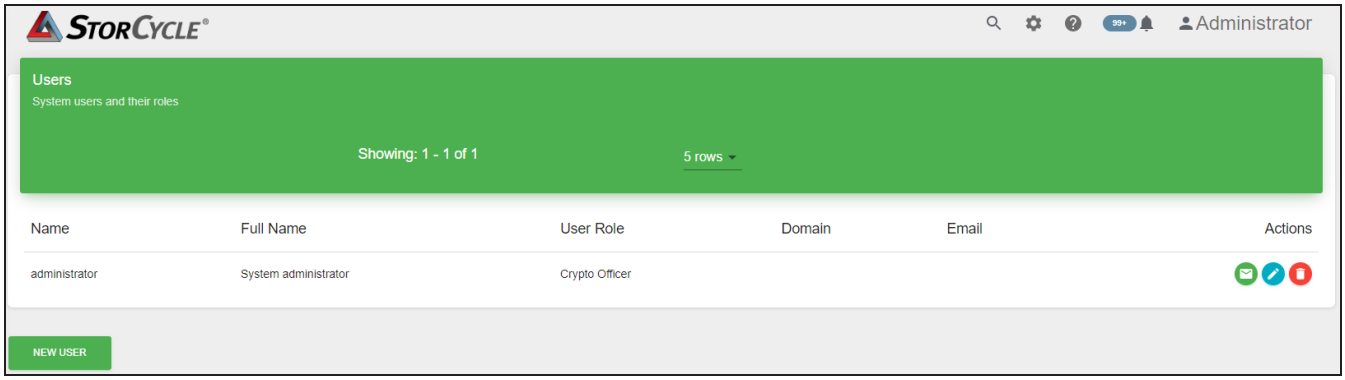


Figure 58 The Users screen.

2. Click **New User**. The New User dialog box displays.

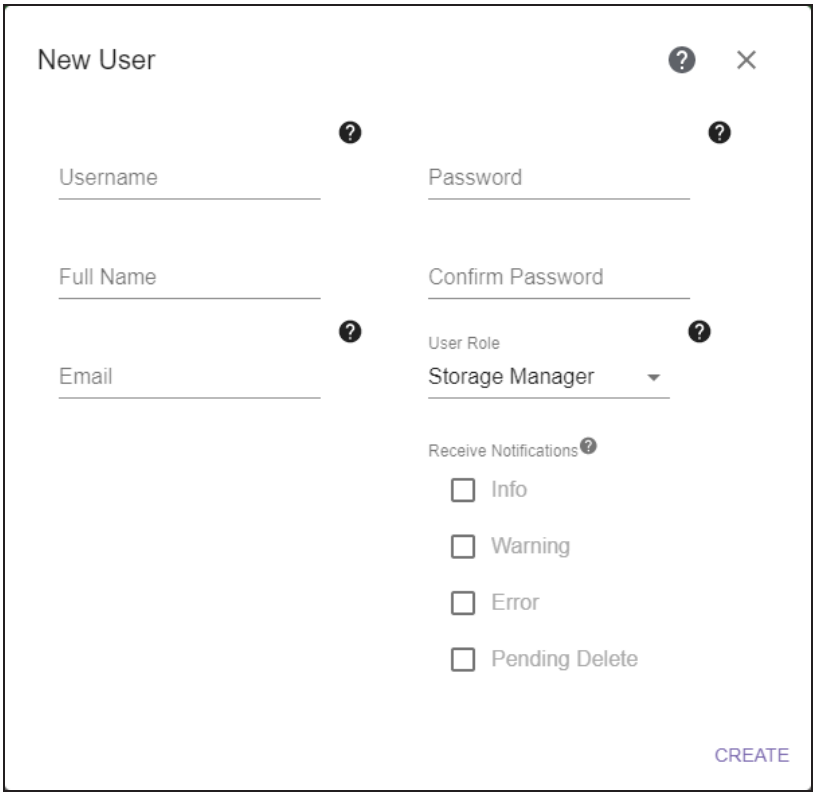


Figure 59 The New User dialog box.

3. Enter the **Username** for the user. If you are using Active Directory Domain user, the username must match the Active Directory user name.

Notes:
- Usernames are NOT case sensitive.
- Usernames must be unique. You cannot have a local user and an Active Directory user with the same username.

4. Enter the user's **Full Name**.
5. Follow one of the following:
   - If Active Directory / LDAP is not configured, continue with Non-Domain User.
   - If the user is not an Active Directory user, continue with Non-Domain User.
   - If Active Directory / LDAP is configured, select a **Domain** and continue with Domain User on page 145.

Non-Domain User

1. If desired, enter an email address for the user. An email address is required if you want the server to send email notifications to this user. SMTP must be configured for the StorCycle solution to send email. See Configure SMTP on page 147.
2. Enter a **Password** and confirm the password. Spectra Logic recommends that the password be at least 8 characters long and contain an upper case letter, a number, and a special character (!@ # $ - = etc.).
3. Enter the role for the user:
   - **Storage Manager** (default)—Storage Managers can view the StorCycle console and migrate and restore data, but cannot change the configuration.
   - **Administrator**—Administrators can access the StorCycle user interface, migrate and restore data, and change the configuration settings, except encryption.
   - **Crypto Officer**— Crypto Officers are Administrators that can also configure encryption.
4. Select the types of notifications to send to the user. The SMTP settings must be configured in order to send emails. See Configure SMTP on page 147.
   - **Info** - An expected event occurred such as a job starting or completing successfully.
   - **Warning** - A job completed with warnings or errors, for example, a file to be migrated / stored was already migrated / stored, therefore, it was skipped. Determine the cause of the problem and remedy it if necessary.
   - **Error** - A job failed with warnings or errors, for example, the StorCycle solution cannot communicate with a storage location. Determine the cause of the error and remedy it as soon as possible.
   - **Pending Delete** - Files are scheduled for deletion from a storage location with a retention policy. Notifications are sent five days prior to file deletion.
5. Click **Submit** to save the user configuration.

Domain User

When you select a domain, the dialog box updates to display the domain user fields.

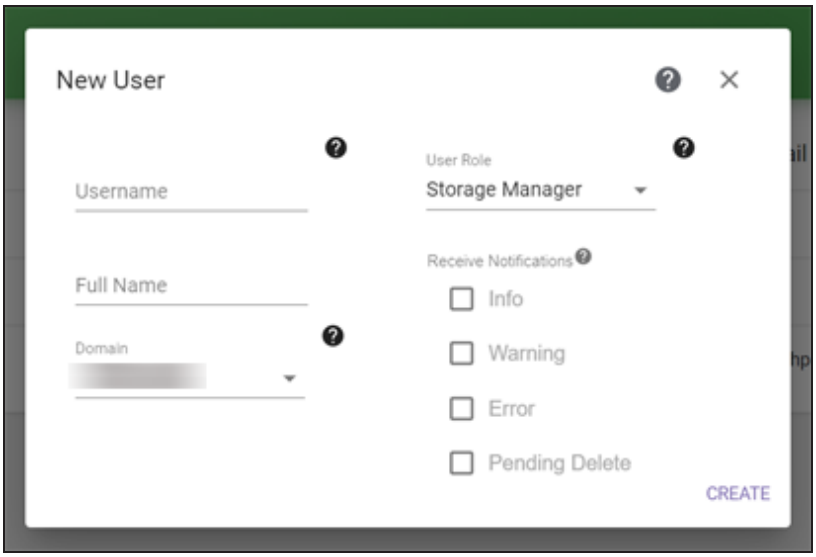


Figure 60 The New User dialog box for a Domain User.

1. Enter the role for the user:
   - **Storage Manager** (default)—Storage Managers can view the StorCycle console and migrate and restore data, but cannot change the configuration.
   - **Administrator**—Administrators can access the StorCycle user interface, migrate and restore data, and change the configuration settings, except encryption.
   - **Crypto Officer**— Crypto Officers are Administrators that can also configure encryption.
2. Select the types of notifications to send to the user. The SMTP settings must be configured in order to send emails. See Configure SMTP on page 147.
   - **Info** - An expected event occurred such as a job starting or completing successfully.
   - **Warning** - A job completed with warnings or errors, for example, a file to be migrated / stored was already migrated / stored, therefore, it was skipped. Determine the cause of the problem and remedy it if necessary.
   - **Error** - A job failed with warnings or errors, for example, the StorCycle solution cannot communicate with a storage location. Determine the cause of the error and remedy it as soon as possible.
   - **Pending Delete** - Files are scheduled for deletion from a storage location with a retention policy. Notifications are sent five days prior to file deletion.
3. Click **Submit** to save the user configuration.

Edit a User

To edit a user, click **Edit** next to the user on the Users screen (see Figure 58 on page 142). Edit the **Full Name**, **Email**, **Password**, **User Role**, and **Notifications** (see Configure Users on page 142 for more information) as desired and click **Update**. If you want to change the username of a user, delete the user and then recreate the user with the new name.

Note: To use the **Send Request to Administrator** HTML links, SMTP must be configured (see Configure SMTP on the next page) and an email address must be configured for the Administrator user.

Send a Test Email

To send a test email to a user, click **Send Test Email** next to the user on the User screen (see Figure 58 on page 142). The email is sent immediately.

Delete a User

To delete a user, click **Delete** next to the user on the User screen (see Figure 58 on page 142). A confirmation screen displays. Click **Delete** to confirm the user deletion.

CONFIGURE SMTP

If desired configure Simple Mail Transfer Protocol (SMTP) to associate the Spectra StorCycle solution with an email server to send messages.

Emails sent from the Spectra StorCycle solution are the first step in troubleshooting issues that may occur. Spectra Logic recommends configuring SMTP and configuring all administrator users to receive emails.

Note: To use the **Send Request to Administrator** option when a user requests a file using HTML links, SMTP must be configured and an email address must be configured for the Administrator user (see Edit a User on the previous page).

Use the instructions below to configure SMTP.

1. Click **Settings** in the toolbar and then select **Configuration > SMTP**. The SMTP screen displays showing the current SMTP settings.

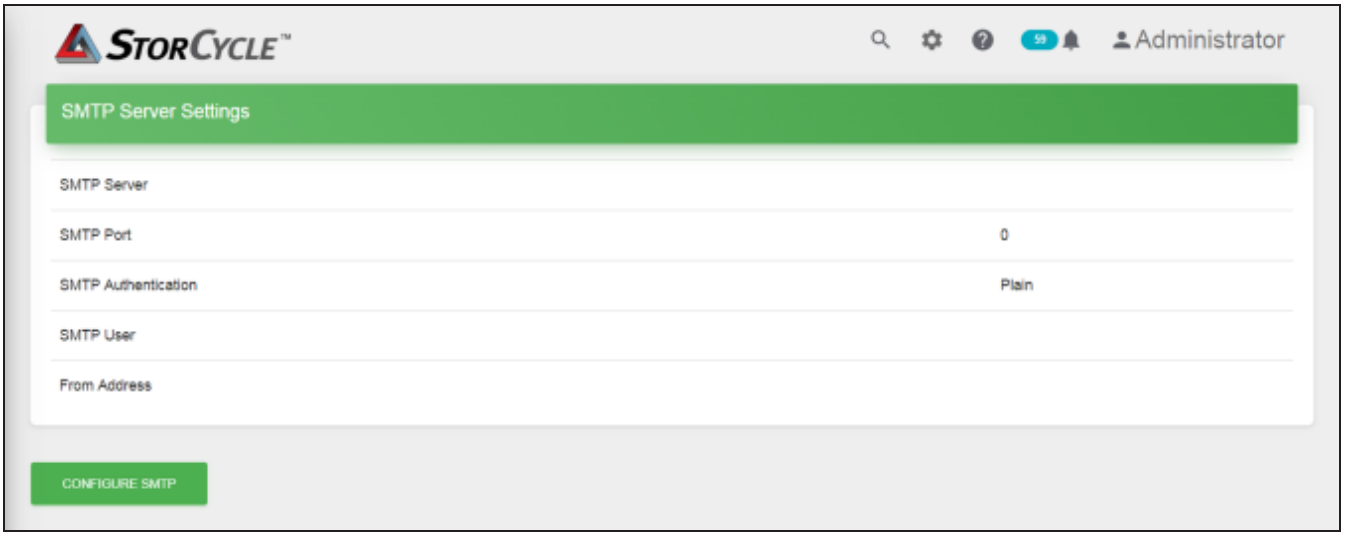


Figure 61 The SMTP screen.

2. Click **Configure SMTP**. The Configure SMTP dialog box displays.

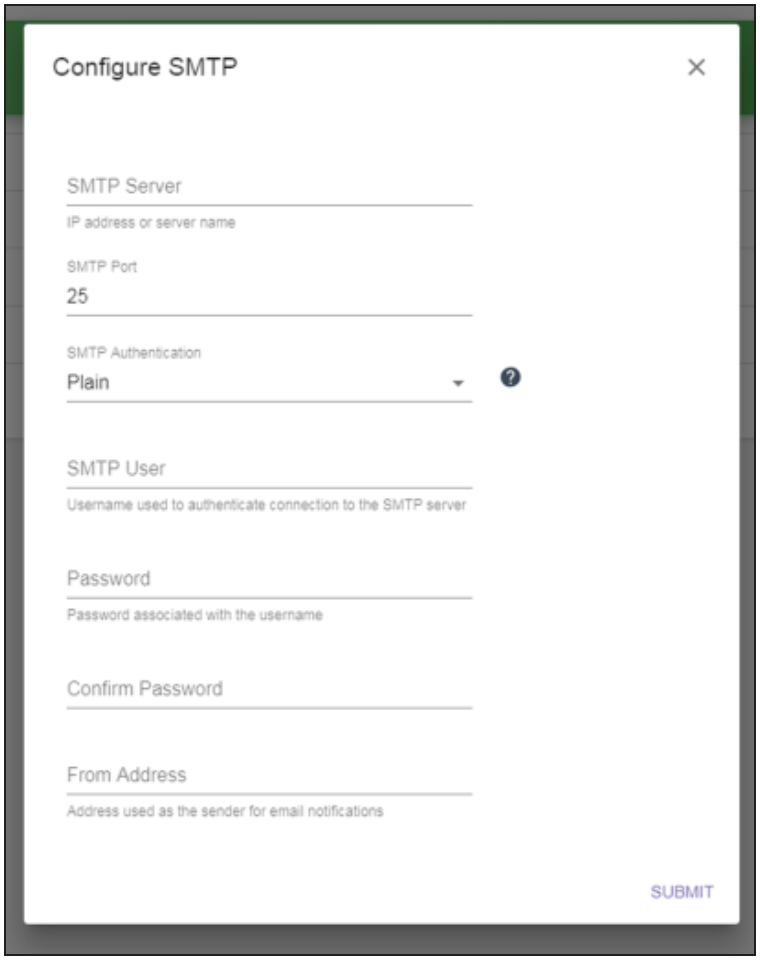


Figure 62 The Configure SMTP dialog box.

3. Enter the IP address or the server name for the **SMTP Server**.
4. Enter the **SMTP Port** to use to connect to the SMTP server.
5. Select **Plain**, **Login**, or **CramMD5** for the **SMTP Authentication** type.
6. In the **SMTP User** field, enter the username used to authenticate connection to the SMTP server.
7. Enter the **Password** associated with the **SMTP User** and confirm the password.
8. In the **From Address** field, enter the email address used as the sender for email notifications.
9. Click **Submit** to save the SMTP configuration.

Chapter 7 - Scan

This section provides instructions for using the Scan wizard.

Scanning Overview

A scan traverses a file system and records, in the StorCycle database, information associated with the directories and files it encounters. A scan can start either at the root of a Storage Location or at a sub-directory of a Storage Location depending on parameters set in the scan project. From the starting directory, the scan traverses all sub-directories beneath it. Once a scan completes, categorization information (age and size of files), for each directory with changes since the last scan of that directory, is updated in the StorCycle database so that you can determine what data to migrate / store based on age and size attributes.

Note: The examples in this section are representations only. The StorCycle solution does not provide reports with similar information.

Scanning from the Root

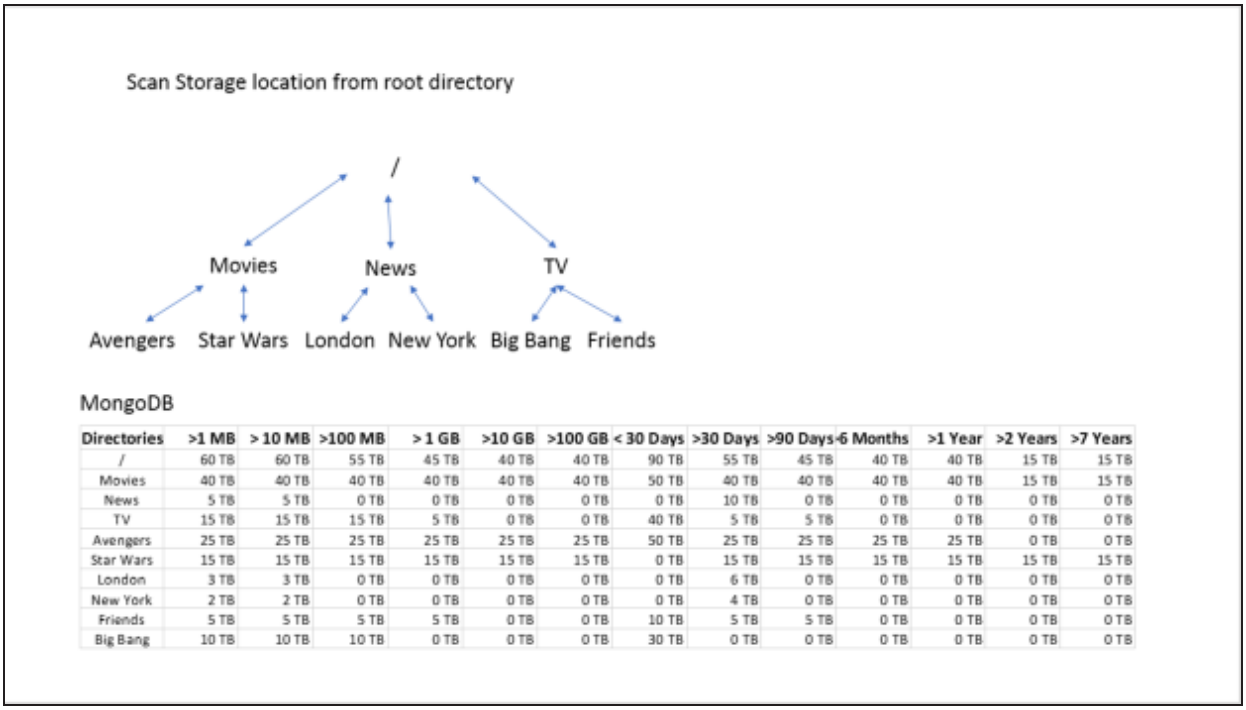
A scan from the root traverses all sub-directories in the Storage Location. If data in a directory has changed since the last time the directory was scanned, the information for the data in the directory is updated in the StorCycle database and the scan histograms. Scanning from the root ensures that the information for all sub-directories is up to date, but it may take a long time.

Scanning from a Sub-Directory

A scan from a sub-directory traverses all sub-directories below the directory selected. If data in a directory has changed since the last time the directory was scanned, the information for the data in the directory is updated in the StorCycle database and histograms for previous scans of parent directories are updated with the new data. A sub-directory scan takes less time than a root scan, but does not update all branches of the storage location.

Example 1 - Scan from Root

A scan starting from the root directory provides the following:



MongoDB

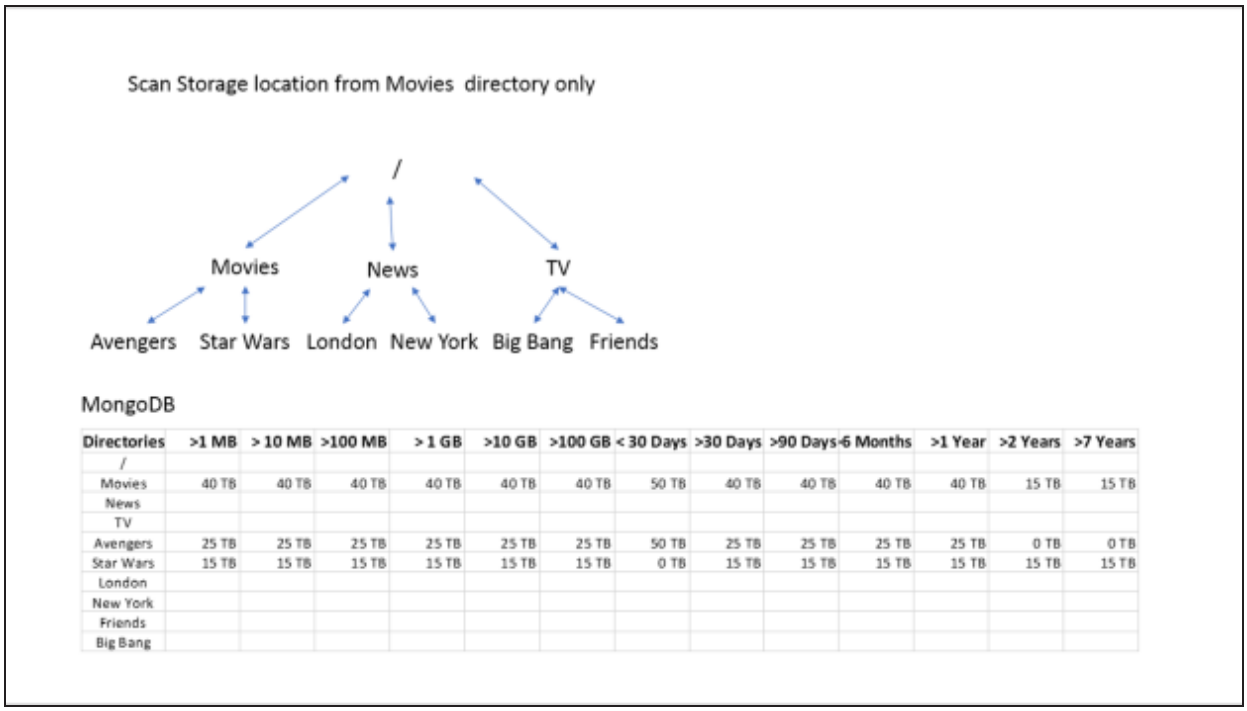
Directories	>1 MB	> 10 MB	>100 MB	> 1 GB	>10 GB	>100 GB	< 30 Days	>30 Days	>90 Days	6 Months	>1 Year	>2 Years	>7 Years
/	60 TB	60 TB	55 TB	45 TB	40 TB	40 TB	90 TB	55 TB	45 TB	40 TB	40 TB	15 TB	15 TB
Movies	40 TB	40 TB	40 TB	40 TB	40 TB	40 TB	50 TB	40 TB	40 TB	40 TB	40 TB	15 TB	15 TB
News	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB	0 TB	10 TB	0 TB	0 TB	0 TB	0 TB	0 TB
TV	15 TB	15 TB	15 TB	5 TB	0 TB	0 TB	40 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Avengers	25 TB	25 TB	25 TB	25 TB	25 TB	25 TB	50 TB	25 TB	25 TB	25 TB	25 TB	0 TB	0 TB
Star Wars	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB	0 TB	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB
London	3 TB	3 TB	0 TB	0 TB	0 TB	0 TB	0 TB	6 TB	0 TB	0 TB	0 TB	0 TB	0 TB
New York	2 TB	2 TB	0 TB	0 TB	0 TB	0 TB	0 TB	4 TB	0 TB	0 TB	0 TB	0 TB	0 TB
Friends	5 TB	5 TB	5 TB	5 TB	0 TB	0 TB	10 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Big Bang	10 TB	10 TB	10 TB	0 TB	0 TB	0 TB	30 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB

Figure 63 An example scan from the root.

Note: When the scan completes, histograms for previous root scans and sub-directory scans for sub-directories traversed by this root scan are updated with the data from the new scan.

Example 2 - Scan from a Sub-Directory

Using the same Storage Location from the last example, a scan starting from the Movies directory traverses and updates the sub-directories shown below:



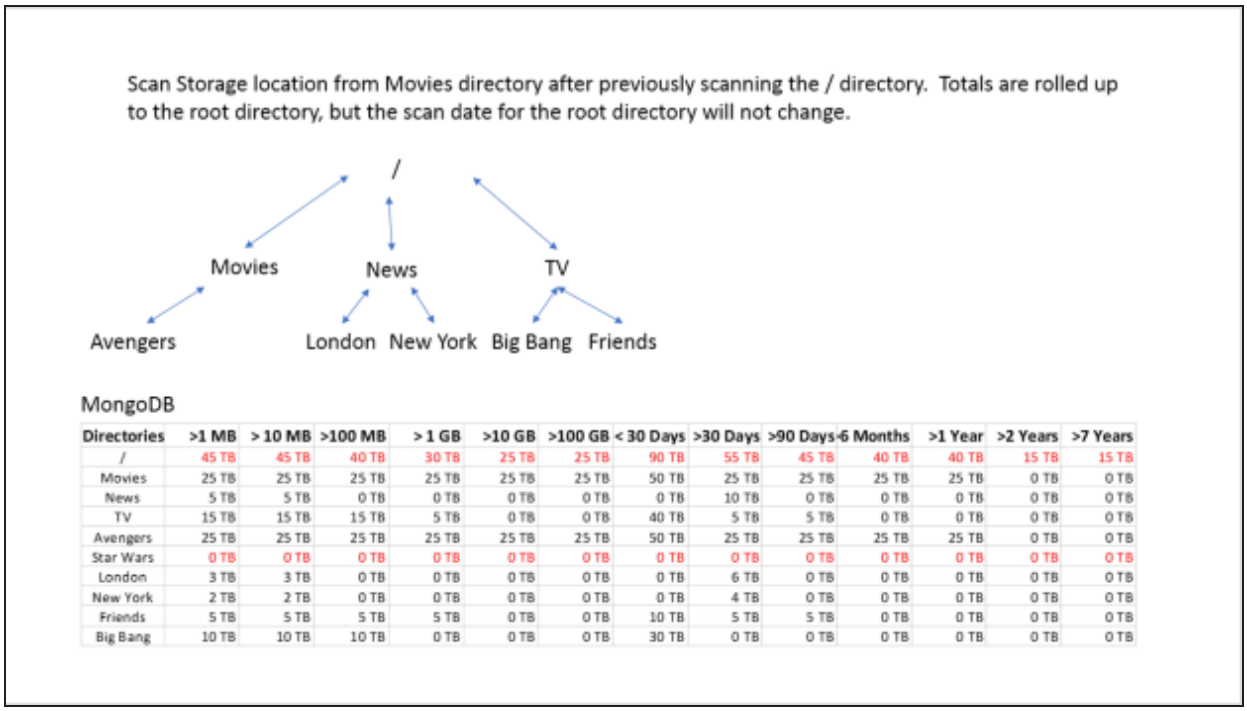
MongoDB

Directories	>1 MB	> 10 MB	>100 MB	> 1 GB	>10 GB	>100 GB	< 30 Days	>30 Days	>90 Days	<6 Months	>1 Year	>2 Years	>7 Years
/													
Movies	40 TB	40 TB	40 TB	40 TB	40 TB	40 TB	50 TB	40 TB	40 TB	40 TB	40 TB	15 TB	15 TB
News													
TV													
Avengers	25 TB	25 TB	25 TB	25 TB	25 TB	25 TB	50 TB	25 TB	25 TB	25 TB	25 TB	0 TB	0 TB
Star Wars	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB	0 TB	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB
London													
New York													
Friends													
Big Bang													

Figure 64 An example scan from a sub-directory.

Example 3 - Scan from a Sub-Directory after Data Deletion

If the Star Wars® files are deleted from the Movies directory, a subsequent scan of the Movies directory updates the root scan as follows:



MongoDB

Directories	>1 MB	> 10 MB	>100 MB	> 1 GB	>10 GB	>100 GB	< 30 Days	>30 Days	>90 Days	6 Months	>1 Year	>2 Years	>7 Years
/	45 TB	45 TB	40 TB	30 TB	25 TB	25 TB	90 TB	55 TB	45 TB	40 TB	40 TB	15 TB	15 TB
Movies	25 TB	25 TB	25 TB	25 TB	25 TB	25 TB	50 TB	25 TB	25 TB	25 TB	25 TB	0 TB	0 TB
News	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB	0 TB	10 TB	0 TB	0 TB	0 TB	0 TB	0 TB
TV	15 TB	15 TB	15 TB	5 TB	0 TB	0 TB	40 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Avengers	25 TB	25 TB	25 TB	25 TB	25 TB	25 TB	50 TB	25 TB	25 TB	25 TB	25 TB	0 TB	0 TB
Star Wars	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB
London	3 TB	3 TB	0 TB	0 TB	0 TB	0 TB	0 TB	6 TB	0 TB	0 TB	0 TB	0 TB	0 TB
New York	2 TB	2 TB	0 TB	0 TB	0 TB	0 TB	0 TB	4 TB	0 TB	0 TB	0 TB	0 TB	0 TB
Friends	5 TB	5 TB	5 TB	5 TB	0 TB	0 TB	10 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Big Bang	10 TB	10 TB	10 TB	0 TB	0 TB	0 TB	30 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB

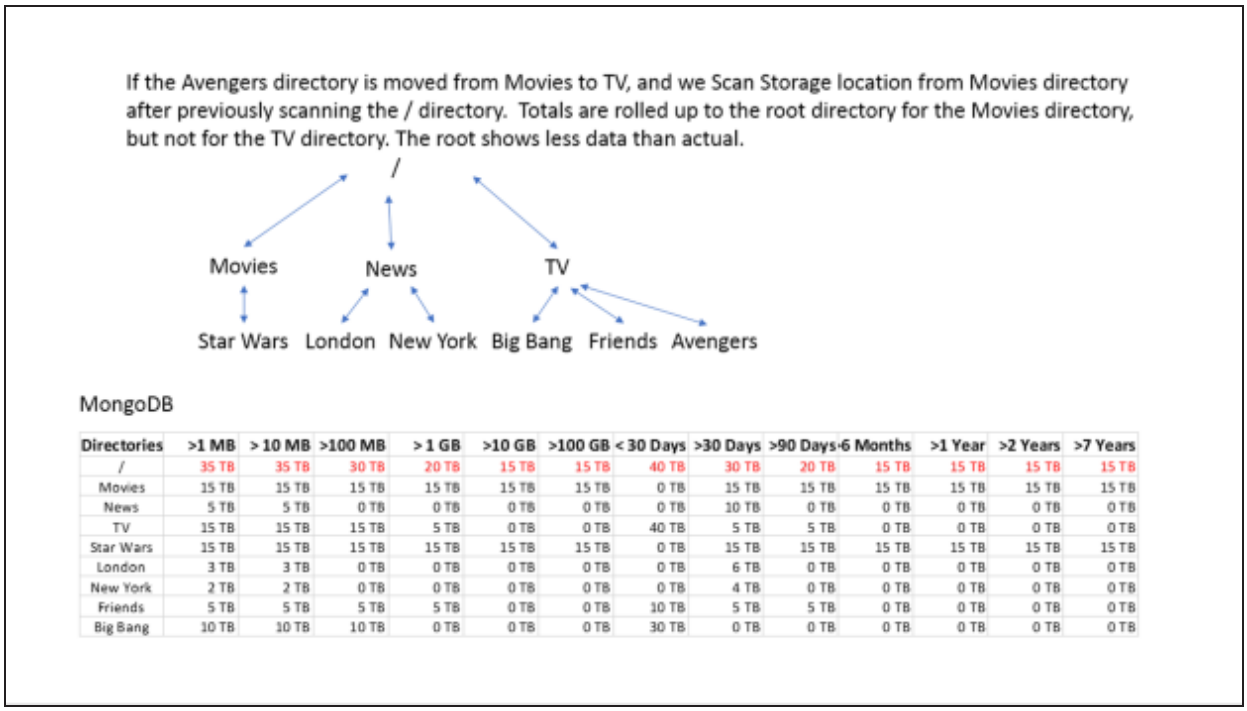
Figure 65 Scan update after data deletion.

Notes:

- This scan updates the parent directory's scan data.
- Old scan data is not re-classified as time passes. What is in the 0 to 30 day category stays there even if enough time has passed that it is now older than 30 days.
- Although this scan updates the data for the root scan, the date of the root scan does not change.

Example 4 - Scan from a Sub-Directory after Data Move

If the Avengers files are moved from the Movies directory to the TV directory, a scan starting from the Movies directory updates the root scan as follows.



Directories	>1 MB	> 10 MB	>100 MB	> 1 GB	>10 GB	>100 GB	< 30 Days	>30 Days	>90 Days	6 Months	>1 Year	>2 Years	>7 Years
/	35 TB	35 TB	30 TB	20 TB	15 TB	15 TB	40 TB	30 TB	20 TB	15 TB	15 TB	15 TB	15 TB
Movies	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB	0 TB	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB
News	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB	0 TB	10 TB	0 TB	0 TB	0 TB	0 TB	0 TB
TV	15 TB	15 TB	15 TB	5 TB	0 TB	0 TB	40 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Star Wars	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB	0 TB	15 TB	15 TB	15 TB	15 TB	15 TB	15 TB
London	3 TB	3 TB	0 TB	0 TB	0 TB	0 TB	0 TB	6 TB	0 TB	0 TB	0 TB	0 TB	0 TB
New York	2 TB	2 TB	0 TB	0 TB	0 TB	0 TB	0 TB	4 TB	0 TB	0 TB	0 TB	0 TB	0 TB
Friends	5 TB	5 TB	5 TB	5 TB	0 TB	0 TB	10 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Big Bang	10 TB	10 TB	10 TB	0 TB	0 TB	0 TB	30 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB

Figure 66 Scan update after data move.

Notes:

- Since the scan started with the Movies sub-directory, it only knows that Avengers is not under Movies any longer. It does not know that it is under TV. The full scan updates to show less data than the Storage Location actually contains. The difference can be corrected by scanning the TV directory or by scanning the root.
- Although this scan updates the data for the root scan, the date of the root scan does not change.

A Migrate / Store Job's Effect on Scan Data

The Migrate / Store wizard shows the latest scan graph for the directory selected as long as a previous root or sub-directory scan included that directory. As shown in Example 4, the latest scan may not be correct. If **Use Last Scan** is selected in the Migrate / Store wizard, the Avengers data will not be considered for Migrating / Storing. To make sure that the correct data is used, select **Scan Before Migrate / Store**.

Notes:
- If **Scan Before Migrate / Store** is selected:
  - The time required to complete the migrate / store job may increase by a significant amount.
- If **Use Last Scan** is selected:
  - Only files present in the directory when the prior scan executed are considered for migration. If the prior scan was for a sub-directory of the working directory, only files in the sub-directory are considered for migration.
  - The current size and age of the file are considered against the selection criteria when determining files to migrate / store.

When the Migrate / Store wizard moves data, it updates all of the directory category totals and the file information for the moved files in the database. This updates the histogram of the scan data for all scans including the affected directories. If the migrate / store used **Use Last Scan**, the database update does not include adding files that were not in the previous scan.

Notes:
- Scan data is not updated after a restore. Similar to adding data to a directory, a new scan, from the root or a sub-directory is required to update the scan results after a restore.
- If you restore objects to their original location, they are not included in future scan data because they are not eligible to be migrated / stored.

Migrate / Store Example

If 30 days after executing Example 4, you choose to migrate / store all files greater than 100 GiB and greater than 6 Months old and select **Use Last Scan**, the database updates as shown after the migrate / store.

Notes:
- The Avengers files were not considered for the migrate / store because they were not included in the previous scan.
- The amount of data greater than 6 months old has increased because the Friends files that were previously greater than 90 days have aged to be greater than 6 months.

If 30 days after doing the Movies scan, you choose to Migrate / Store all files > 1 GB and > 6 Months old and select **Use Previous Scan**, the database updates as shown after the migrate / store. The Avengers directory was never considered for migrate / store because it was not in the previous scan.

MongoDB

Directories	>1 MB	> 10 MB	>100 MB	> 1 GB	>10 GB	>100 GB	< 30 Days	>30 Days	>90 Days-6 Months	>1 Year	>2 Years	>7 Years
/	35 TB	35 TB	30 TB	15 TB	5 TB	5 TB	40 TB	30 TB	15 TB	10 TB	15 TB	15 TB	0 TB
Movies	15 TB	15 TB	15 TB	15 TB	5 TB	5 TB	0 TB	15 TB	15 TB	10 TB	15 TB	15 TB	0 TB
News	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB	0 TB	10 TB	0 TB	0 TB	0 TB	0 TB	0 TB
TV	15 TB	15 TB	15 TB	5 TB	0 TB	0 TB	40 TB	5 TB	5 TB	0 TB	0 TB	0 TB	0 TB
Star Wars	15 TB	15 TB	15 TB	15 TB	5 TB	5 TB	0 TB	15 TB	15 TB	10 TB	15 TB	15 TB	0 TB
London	3 TB	3 TB	0 TB	0 TB	0 TB	0 TB	0 TB	6 TB	0 TB	0 TB	0 TB	0 TB	0 TB
New York	2 TB	2 TB	0 TB	0 TB	0 TB	0 TB	0 TB	4 TB	0 TB	0 TB	0 TB	0 TB	0 TB
Friends	5 TB	5 TB	5 TB	0 TB	0 TB	0 TB	10 TB	5 TB	0 TB	0 TB	0 TB	0 TB	0 TB
Big Bang	10 TB	10 TB	10 TB	0 TB	0 TB	0 TB	30 TB	0 TB	0 TB	0 TB	0 TB	0 TB	0 TB

Note: For this example, the Friends files that were previously > 90 days have aged to be greater than 6 months.

Figure 67 Scan update after a migrate / store.

CREATE A SCAN PROJECT

Configure a scan project to evaluate data in primary storage to determine the possible savings available if older files are moved to secondary storage.

Notes:
- Only 10 concurrent scans are allowed.
- You cannot create a scan project for a storage location that is offline.

Use the instructions below to configure a new scan project.

1. Click **Scan** in the taskbar. The Scan screen displays showing configured recurring and single run scan projects and current and completed scan jobs.

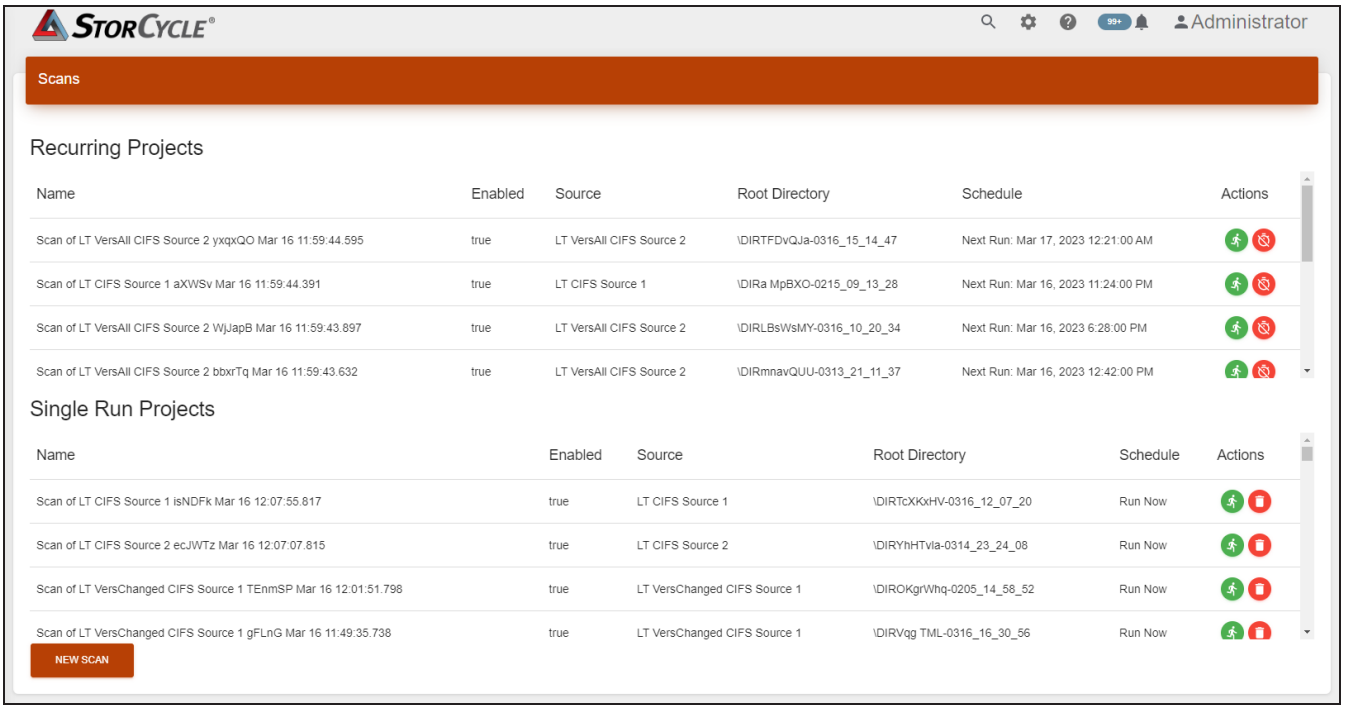


Figure 68 The Scan screen.

2. Click **New Scan** to start the Scan wizard.

Scan Wizard—Scan Source

The Scan Source screen of the Scan wizard allows you to configure the scan name and scan source.

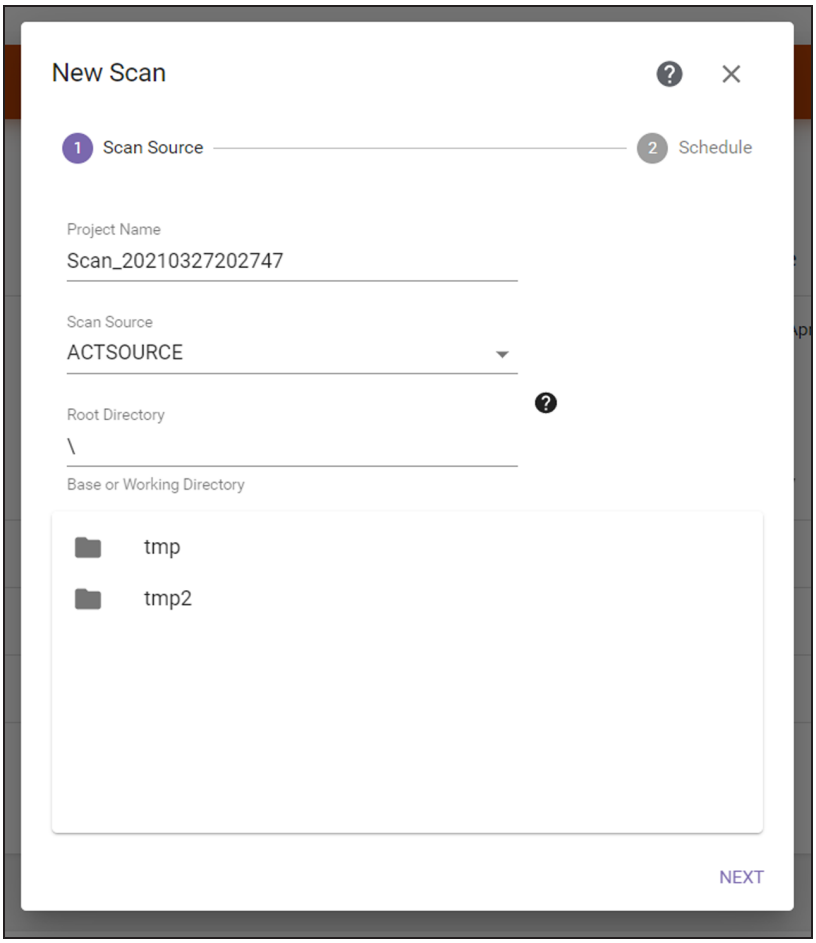


Figure 69 The Scan Source screen of the Scan wizard.

1. If desired, edit the **Project Name** for the scan.

IMPORTANT A project name must be unique across all scan, migrate / store, restore, and database backup projects. Names of deleted projects cannot be reused.

2. From the **Scan Source** drop-down, select a previously configured storage location (see Storage on page 81) or select **Create New Source** and enter a name and the UNC path to create a new Non-Spectra NAS storage location.

Notes:
- Only storage locations configured as a Source storage location type are listed in the drop-down.
- **Create New Source** is only available for an Administrator user.
- The storage location created with **Create New Source** has the following defaults:
  - Storage Type: Non-Spectra NAS
  - Storage Location Type: Source
  - Description: Created for project: <project_name>
  - Department and Cost/TiB: blank
  - Do Not Limit Transfer During Peak Hours

3. If you are using a previously configured storage location, you can select a sub-directory on the source as the starting point (**Root Directory**) for the scan.
4. Click **Next** to continue.

Scan Wizard—Schedule

The Schedule screen of the Scan wizard allows you to configure when to run the scan project.

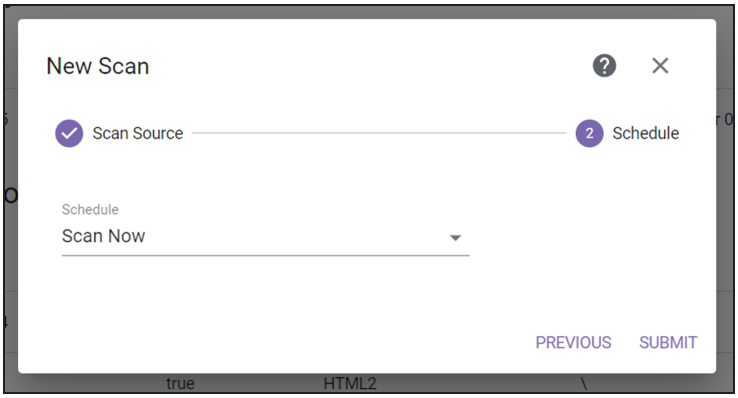


Figure 70 The Schedule screen of the Scan wizard.

Select Scan Now on the next page, Set Start Time on the next page, or Set Recurring Schedule on page 161 to set the run schedule.

Scan Now

Click **Submit** to save the project. The scan runs immediately.

While the job is active, hovering over the total bytes for the job in the Scan Jobs section of the Scan screen displays the scan performance, see Figure 117 on page 230.

Set Start Time

If you select **Set Start Time**, the dialog box updates to display the following fields:

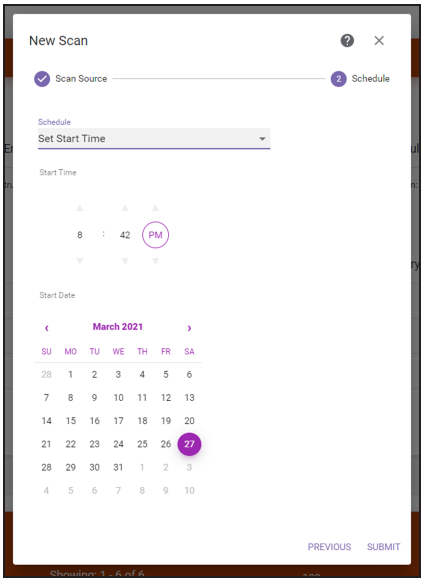


Figure 71 Setting a start time.

1. Use the up and down arrows to select the **Start Time** for executing the scan.
2. Using the calendar, select the **Start Date** on which to execute the scan.
3. Click **Submit** to save the project. The job runs as scheduled.

While the job is active, hovering over the total bytes for the job in the Scan Jobs section of the Scan screen displays the scan performance, see Figure 117 on page 230.

Set Recurring Schedule

If you select **Set Recurring Schedule**, the dialog box updates to display the following fields:

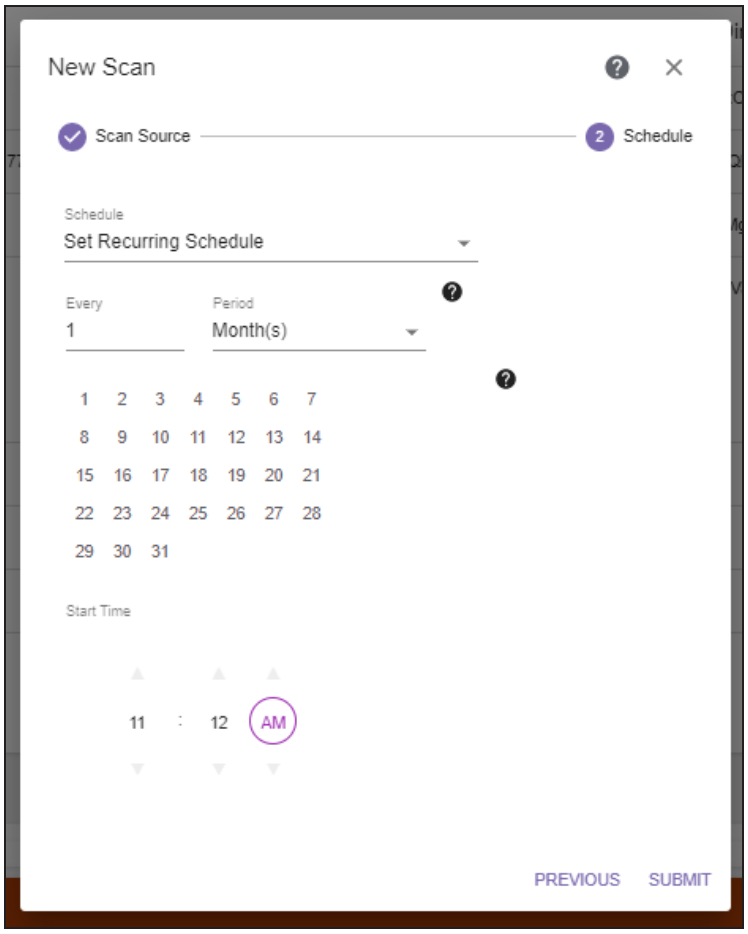


Figure 72 Setting a recurring schedule.

1. Select on what **Period** (weekly, monthly) to execute tasks associated with this project.
   - If you selected **Weekly**, select the day of the week on which to execute the scan.
   - If you selected **Monthly**, select the day of the month on which to execute the migrate / store job. If you select a day of the month that is not valid for all months (for example, the 31st), the last day of the month is used in shorter months.
2. Specify the **Interval**, of weeks or months, before the next execution of a scan. For example, if this value is set to 1, the action occurs every week or month, if the value is set to 2 the action occurs every other week or month, etc.
3. Use the up and down arrows to select the **Start Time** for executing the scan.
4. Click **Submit** to save the project. The job runs as scheduled.

While the job is active, hovering over the total bytes for the job in the Scan Jobs section of the Scan screen displays the scan performance, see Figure 117 on page 230.

Pause a Scan Project

Pausing a scan project stops a project with a recurring schedule, or a single run project scheduled for the future, from running. It does not remove the project from the list of projects on the Scan screen (see Figure 68 on page 157).

Note: Pausing a project does not cancel a job that is currently running. To cancel a scan job that is queued, verifying, or active, see Cancel a Scan Job below.

To pause a scan project, click **Pause** next to the project that you want to pause. In the Pause or Disable window, select **Pause Project Schedule** from the Choose Action drop-down list, and click **Submit**.

To resume the paused project, see Resume a Scan Project below.

Resume a Scan Project

Resuming a scan project restarts the schedule for a project with a recurring schedule or a single run project scheduled to run in the future.

Note: If the current time is past the scheduled run time for a single run project, the job does not run when resumed.

To resume a scan project, click **Resume** next to the project that you want to resume (see Figure 68 on page 157). In the Resume or Disable window, select **Resume Project Schedule** from the Choose Action drop-down list, and click **Submit**. The project will run at the next scheduled time.

Cancel a Scan Job

To cancel a queued, verifying, or active scan job, click **Cancel** next to the job on the Scan screen (see Figure 68 on page 157) or the Active and Completed Jobs screen (see Figure 116 on page 230). A confirmation screen displays. Click **Cancel Job** to confirm the cancellation. When a scan is canceled, no changes are made to previous scan data.

Disable a Scan Project

Disabling a scan projects stops a project with a recurring schedule, or a single run project scheduled for the future, from running and removes it from the list of projects on the Scan screen (see Figure 68 on page 157).

Note: Disabling a project does not cancel a job that is currently running. To cancel a scan job that is queued, verifying, or active, see Cancel a Scan Job on the previous page.

To disable a scan project, do one of the following:

- For a single run project, click **Disable** next to the project on the Scan screen (see Figure 68 on page 157). A confirmation screen displays. Click **Delete** to confirm disabling the project.
- For a Recurring project, click **Pause** or **Resume**, select **Disable Project** from the **Choose Action** drop-down list. A confirmation screen displays. Click **Submit** to confirm disabling the project.

  Note: Even after disabling the project, the project name cannot be reused.

Chapter 8 - Migrate or Store Data

This section provides instructions for using the Migrate / Store wizard.

MIGRATE / STORE OVERVIEW

A Migrate / Store project moves scanned data from primary storage to secondary storage. When configuring a new Migrate / Store project, if a scan was previously done, StorCycle graphically displays all scanned data within the selected storage location by file size and age. This allows a user to easily select to move all scanned files or only a portion based on particular file sizes or file age from primary storage to a lower-cost storage medium.

File age is the most important property for determining which files should be migrated. The older the file, the less likely that it is to be accessed. File age is typically determined by the date the file was last accessed, but StorCycle also optionally allows file age to be based on the last modified date or creation date of the file. To change the basis for file age, see Configure Global Settings on page 135.

File size is also important for determining which files to migrate:

- Migration of smaller files from primary storage does not have as big of an impact on freeing up space and improving performance when compared to moving large files.
- Small files transfer to secondary storage at a slower rate (MiB/s) than large files.
- Small files have a larger impact on the count of files/objects in object storage. Object storage systems like the Spectra BlackPearl system typically have an object count maximum. Packing, described in Configuring Storage on page 89, can address this issue.

Using Scan Results for Migration

When migrating data, users have the choice of whether to scan before migrating.

- **Scan before Migrate / Store** — Perform a new scan, and then migrate files that meet the specified criteria for age and size. Use this option if a prior scan result is not available, if it has been a long time since the latest scan, or if there has been a large content change in the storage location.
- **Use Last Scan** — Migrate files that meet the specified criteria for age and size based on the most recent scan result. This is the most efficient choice.

Create a Migrate / Store Project

Configure a migrate / store project to find and move objects to secondary storage.

Understanding Migrate / Store Project Functionality

Use the information in this section to understand the behavior of certain aspects of a migrate / storage project that may apply to your storage environment.

Directories

- When the StorCycle solution migrates / stores or restores files, it also migrates / stores or restores associated directories. While the StorCycle solution ensures that a file does not already exist on the target and does not overwrite the file, it may overwrite existing directories.
  - When the Windows version of the StorCycle solution overwrites a directory, it resets the permissions / ACLs based on the permissions / ACLs that are on the directory that it is migrating.
  - When the Linux version of the StorCycle solution overwrites a directory, it does not reset the permissions / ACLs (because Linux does not have an "Auto Inherit" flag like Windows).
- The StorCycle solution migrates / stores empty directories.
- Having the target directory for a migrate / store job open in Windows Explorer may cause "The process cannot access the file because it is being used by another process" errors.

Previously Migrated Files

- The StorCycle solution does not migrate / store files that have been previously migrated / stored, even if the file has changed on the source storage location. If you want to migrate / store the file again, you must first move it to another path location.

File Extended Attributes

- The StorCycle solution migrates / stores and restores the access, created, and modified times, and the DACLs (Windows or Linux) or group/owner/mode (Linux). For BlackPearl and S3 targets, these attributes are added to the objects as metadata.
- The StorCycle solution does not migrate / store Alternative Data Streams or SACLs.
- For Linux systems, extended attributes (xattr) are migrated / stored and restored. Since the value of an extended attribute may include binary data, the StorCycle solution encodes the data in base64.

Symbolic or HTML Links

- When the StorCycle solution migrates / stores symbolic links to Spectra or non-Spectra NAS, they are migrated / stored as a text file containing the symbolic link path, even if the target does not support symbolic links. The symbolic link on the source is replaced by a StorCycle link (HTML link or symbolic link) if you selected one of these options.
- When the StorCycle solution migrates / stores symbolic links to a BlackPearl system or S3 storage location, they are migrated / stored as a zero byte object, with the symbolic link path stored in the object metadata. The symbolic link on the source is replaced by a StorCycle link (HTML link or symbolic link) if you selected one of these options.
- When the StorCycle solution migrates / stores symbolic links to an Amazon Glacier storage location, no object is stored in Amazon Glacier, however the symbolic link path is stored by the StorCycle solution. The symbolic link on the source is replaced by a StorCycle link (HTML link or symbolic link) if you selected one of these options.

Create a Migrate / Store Project

Use the instructions below to configure a new migrate / store project.

IMPORTANT The StorCycle solution requires that daily database backups are configured and scheduled before any migrate / store jobs can be created.

1. Click **Migrate / Store** in the taskbar. The Migrate / Store screen displays showing configured recurring and single run migrate / store projects and current and completed migrate / store jobs.

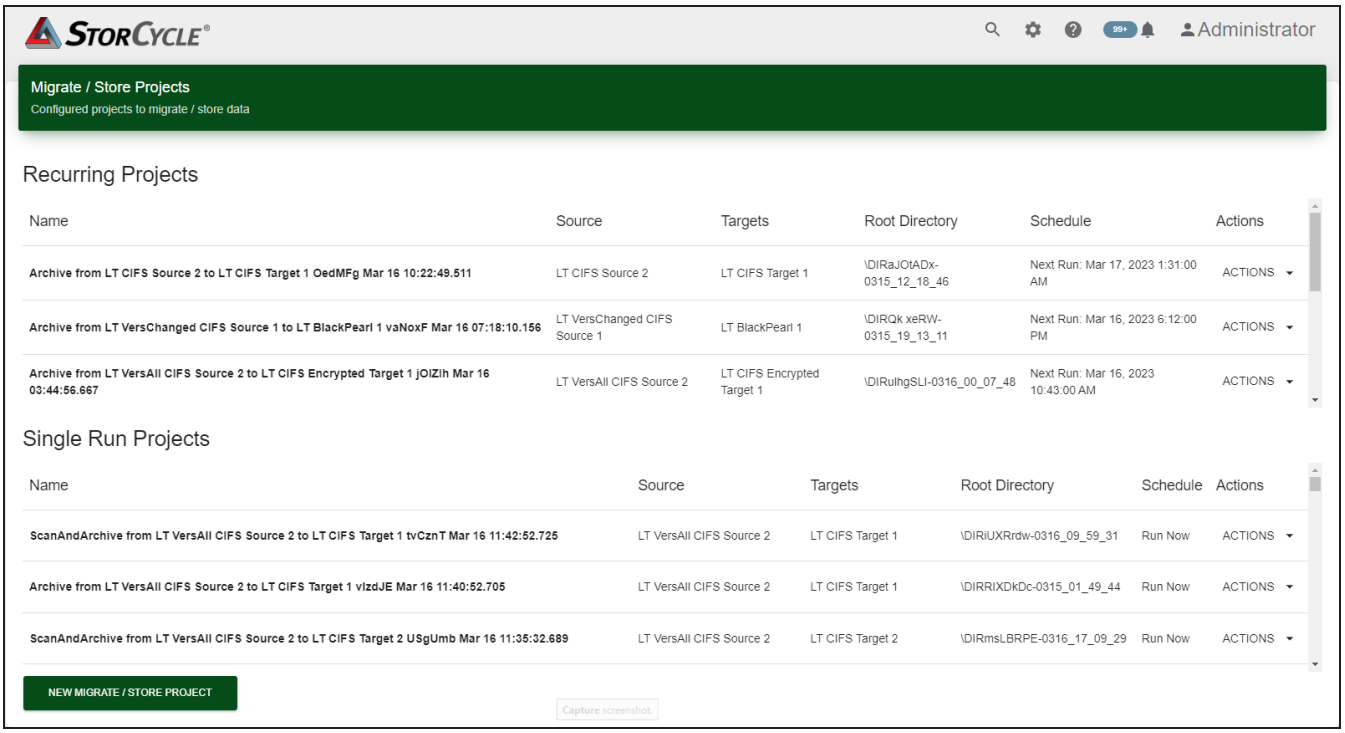


Figure 73 The Migrate / Store screen.

2. Click **New Migrate / Store Project** to start the Migrate / Store wizard.

Migrate / Store Wizard—Project Name

The Project Name screen of the Migrate / Store wizard allows you to configure the project name and storage location.

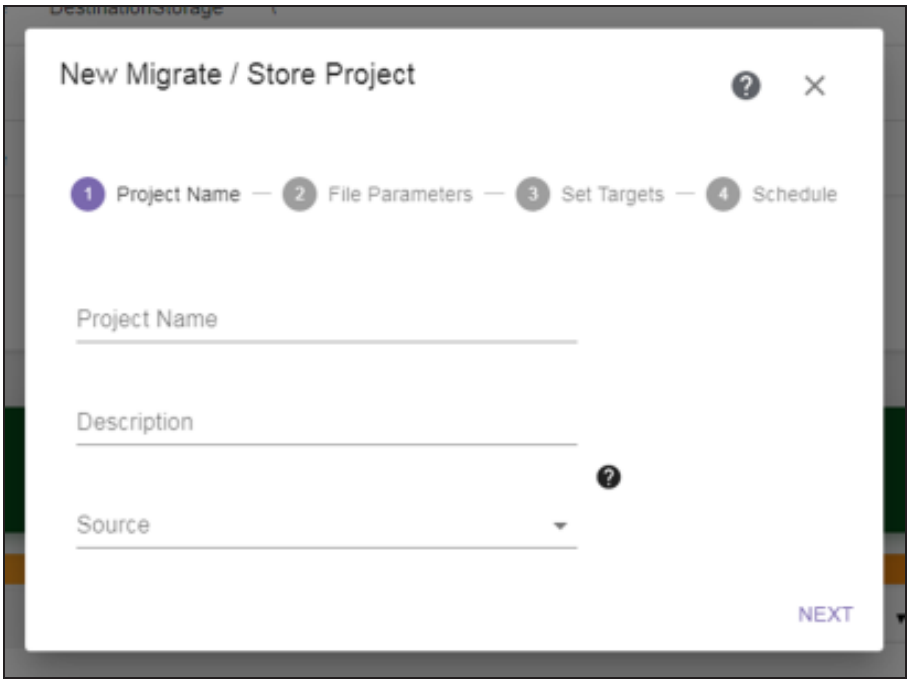


Figure 74 The Project Name screen of the Migrate / Store wizard.

1. Enter a unique **Project Name** for the project.

IMPORTANT

A project name must be unique across all Scan, Migrate / Store, Restore, and Database Backup projects. Names of deleted projects cannot be reused.

The name of a Migrate / Store project can be used to search for the project and associated files.

2. If desired, enter a **Description** for the project.

3. From the **Source** drop-down, select a previously configured storage location (see Storage on page 81) to be the source location or select **Create New Source** and enter a name and the UNC path to create a new Non-Spectra NAS storage location. Sub-directories on the Source display.

Notes:
- Only storage locations configured as a Source storage location type are listed in the drop-down.
- **Create New Source** is only available for an Administrator user.
- The storage location created with **Create New Source** has the following defaults:
  - Storage Type: Non-Spectra NAS
  - Storage Location Type: Source
  - Description: Created for project: <project_name>
  - Department and Cost/TiB: blank
  - Do Not Limit Transfer During Peak Hours

4. If you are using a previously configured storage location, you can select a sub-directory on the source as the starting point (**Root Directory**) for searching for objects to Migrate / Store.
5. Click **Next** to continue.

Migrate / Store Wizard—File Parameters

The File Parameters screen of the Migrate / Store wizard allows you to configure filters to select the files to migrate or store.

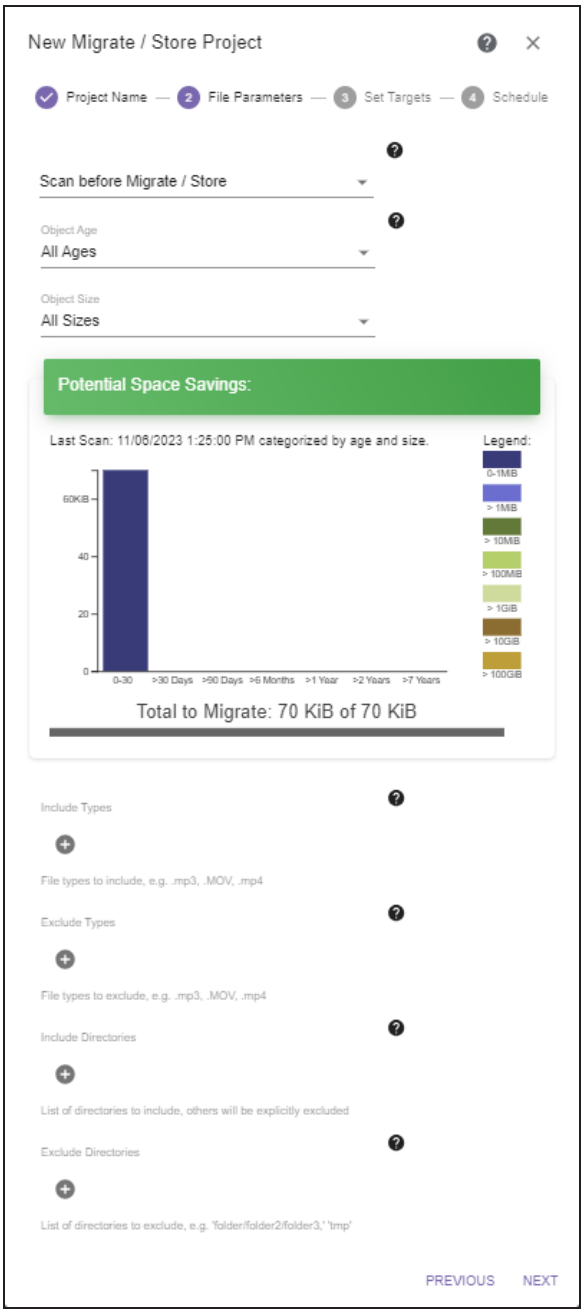


Figure 75 The File Parameters screen of the Migrate / Store wizard.

Use the instructions below to set file parameters.

1. Select whether to **Scan before Migrate / Store** or to **Use Last Scan** to determine the files to migrate / store.

- **Scan before Migrate / Store** — Perform a new scan, and then migrate files that meet the specified criteria for age and size. Use this option if a prior scan result is not available, if it has been a long time since the latest scan, or if there has been a large content change in the storage location. This is the default.

Note: Only files present in the working directory when the prior scan executed are considered for migration.

- **Use Last Scan** — Migrate files that meet the specified criteria for age and size based on the most recent scan result.

Note: If there is a previous scan for one or more sub-directories of the working directory, this option is available, but only the files in the scanned directories are considered for migration.

2. From the **Object Age** drop-down, select the age of files to include or, if desired, select **Custom (days)**. If you selected **Custom (days)**, enter the number of days. All files older than the entered number of days are included.

Notes:
- **Object Age** is determined using the configured **Method to determine file age**. See Configure Global Settings on page 135 for more information.
- Only those objects meeting the **Object Age** and the **Object Size** requirements are included.
- The Potential Space Saving graph updates to indicate the potential space savings based on the **Object Age** selection.
- Custom object ages do not display in the histogram.

3. From the **Object Size** drop-down, select size of files to include.

Notes:
- Only those objects meeting the **Object Age** and the **Object Size** requirements are included.
- The Potential Space Saving graph updates to indicate the potential space savings based on the **Object Size** selection.

4. If desired, select file types to include, file types to exclude, or directories to exclude.
   - Under **Include Types**, click the plus (+) sign to add a new line for entering a file extensions for file types to include. Specifying file types here excludes all file types not listed.
   - Under **Exclude Types**, click the plus (+) sign to add a new line for entering a file extensions for file types to exclude. Specifying file types here includes all file types not listed.
   - Under **Include Directories**, click the plus (+) sign to add a new line for entering directories to include.
   - Under **Exclude Directories**, click the plus (+) sign to add a new line for entering directories to exclude.

Notes:
- The Potential Space Saving graph does not update based on **Includes Types**.
- File extensions are case sensitive.
- Entering both **Include Types** and **Exclude Types** applies **Exclude Types** before **Include Types**.
- The **Include Type**, **Exclude Type**, **Include Directories**, and **Exclude Directories** fields support regular expressions, including those shown below:

Character	Definition	Example	Match
. (dot)	Matches any single character, equivalent to ? (question mark) in wild card expressions.	ss.	ssa, ssb, ssc
\ (backslash)	Is used as an "escape" character to protect a subsequent special character.	\%	%
.* (dot and asterisk)	Matches any string, equivalent to * in standard wild card expressions.	st.*	storcycle, st, stop
* (asterisk)	The proceeding item is repeated zero or more times.	a*	a, aa, aaa
[ ] (square brackets)	Specifies a range of matches.	m[a,o,u]m	mam, mom, mum
[^] (caret in square brackets)	Performs a logical “not”, equivalent of [!] in standard wild cards.	file[^3]	file1, file2, file4
^ (caret)	Matches expression at start of string.	^The	any string that starts with The
$ (dollar sign)	Matches expression at end of string.	end$	any string that ends with end

5. Click **Next** to continue.

Migrate / Store Wizard—Set Targets

The Set Targets screen of the Migrate / Store wizard allows you to configure the target storage location for the Migrate / Store project and specify the replacement option on the source.

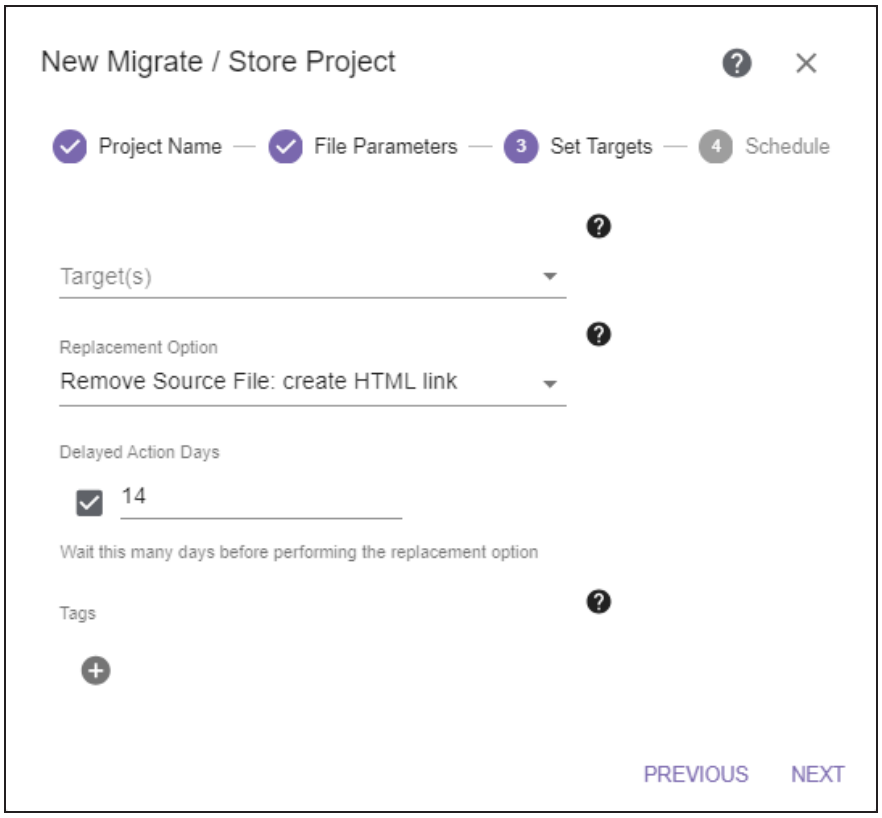


Figure 76 The Set Targets screen of the Migrate / Store wizard.

1. From the **Target(s)** drop-down menu, select up to three previously configured storage locations. See Storage on page 81 for instructions for configuring a storage location.

CAUTION

Do not configure multiple source storage locations to migrate / store to the same NAS target storage location, such that the directory and file names could conflict on the target. For example, if Storage Locations A and B both contain a top-level directory **dir1** which contains a file named **file1.txt**, and the file from both locations are migrated to the same NAS target, the migrate / store operation fails.

IMPORTANT

Spectra Logic recommends making two copies of migrated data in two geographically-separated locations. This can be done by selecting two targets in the StorCycle Migrate / Store wizard or by selecting a BlackPearl system with data policy set to migrate data to any combination of tape, disk, and cloud.

For more information on multiple geographically-separated data copies, see StorCycle Quick Reference on page 25.

IMPORTANT To replace migrated / stored files with symbolic links, the migrate / store project must have only one NAS target. Additional BlackPearl or S3 targets are optional.

Notes:
- If the source is an S3 storage location, the target must be a BlackPearl storage location that does not have packing enabled.
- You cannot mix encrypted targets and unencrypted targets in a single migrate / store project.

2. Select the **Replacement Option** for the files after they are copied to secondary storage. All selections for Replacement Option result in the StorCycle solution tracking migrated files in the StorCycle database, and allows the files to be restored.

IMPORTANT If the NAS target storage location has a retention policy set and you select **Remove Source File: create Symbolic link** or **Remove Source File: create HTML link** then the links are removed from the source when the files are removed from the NAS target.

Note: When a migrate / store project is configured to delete the source file, or replace the source file with an HTML or symbolic link, the StorCycle solution checks the file timestamp and size to ensure that the file has not changed between the time it was migrated / stored and when it is deleted or replaced. If the file changed during this time, then the file is not deleted or replaced from the source storage, and a note is added to the job logs.
- If the source is an S3 storage location, you cannot replace the files with HTML or Symbolic links.
- If the targets are encrypted storage locations, you cannot replace the files with Symbolic links.

- **Keep Source File** —The original copy of the object is kept in primary storage.
- **Remove Source File: no links**—The original copy of the object is removed from primary storage. The directory structure is left in place. The empty directories can be deleted. Upon restore, any missing directories will be recreated.
- **Remove Source File: create Symbolic link**—The original copy of the object is replaced with a symbolic link which transparently opens the file from secondary storage.

Notes:
- To replace migrated / stored files with symbolic links, the migrate / store project only supports using one NAS target. Additional BlackPearl or S3 targets are optional.
- If the source is an S3 storage location, you cannot replace the files with Symbolic links.
- If the targets is an encrypted storage location, you cannot replace the files with Symbolic links.

- **Remove Source File: create HTML link**—The original copy of the object is replaced with an HTML link with instructions for restoring the file from secondary storage.

Notes:
- If the network does not support reverse DNS lookups, then the IP address of the storage location is used in the HTML link created during a Migrate / Store job.
- If you entered a **Hostname Override** (see Configure Global Settings on page 135), the URL entered is used in the HTML link created during a Migrate / Store job.
- If the source is an S3 storage location, you cannot replace the files with HTML links.

- **Remove Source Files and any Empty Directories**—The original copy of the object is removed from primary storage. Any empty directories are deleted. Upon restore, any missing directories will be recreated.
- **Remove Source Files: replace with single HTML link**—An HTML link to restore the entire project is placed in the project's root directory and all files are removed.

Notes:
- If the network does not support reverse DNS lookups, then the IP address of the storage location is used in the HTML link created during a Migrate / Store job.
- If you entered a **Hostname Override** (see Configure Global Settings on page 135), the URL entered is used in the HTML link created during a Migrate / Store job.
- If the source is an S3 storage location, you cannot replace the files with HTML links.

3. If desired, under **Delay Action Days**, select the check box to set a delay timer in days to remove the object from the source.
4. If desired, under **Tags**, click the plus (+) sign to add a new line for entering tags to apply to this task for searching purposes. Search by Tag allows you to search for any sub string within the tag. See Search by Tag on page 197 for more information.
5. Click **Next** to continue.

Migrate / Store Wizard—Schedule

The Schedule screen of the Migrate / Store wizard allows you to configure when to run the migrate / store project.

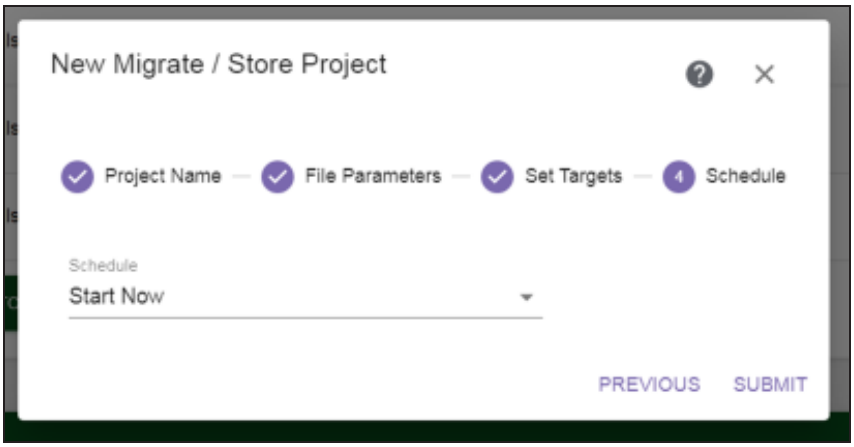


Figure 77 The Schedule screen of the Migrate / Store wizard.

- Using the **Schedule** drop-down menu, select **Start Now**, **Set Start Time**, or **Set Recurring Schedule** to set the run schedule.
- If you selected **Start Now**, click **Submit** to save the project. The project starts immediately.

  While the job is active, hovering over the total bytes for the job in the Migrate / Store Jobs section of the Migrate / Store screen displays the migrate / store performance, see Figure 117 on page 230.
- If you selected **Set Start Time** or **Set Recurring Schedule**, the dialog box updates to show the configuration fields required for that schedule type. Continue with the applicable section below:
  - Set Start Time on the next page
  - Set Recurring Schedule on page 179

Set Start Time

If you select **Set Start Time**, the dialog box updates to display the following fields:

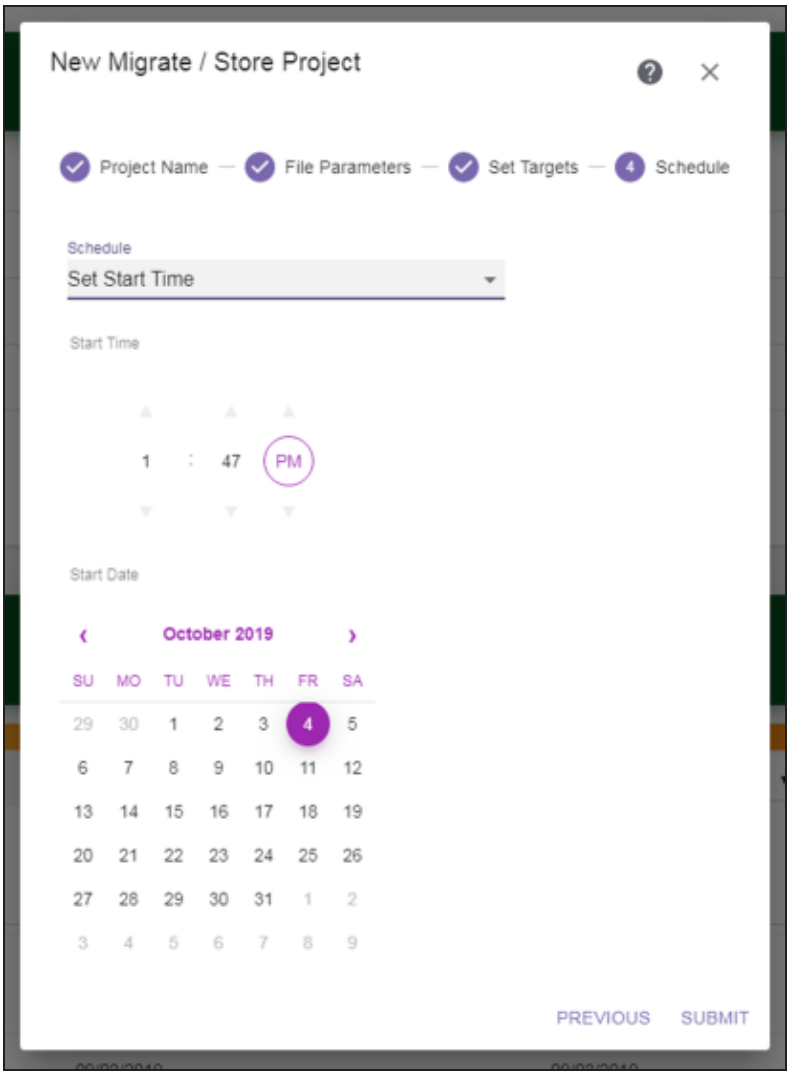


Figure 78 Setting a start time.

1. Use the up and down arrows to select the **Start Time** for executing the migrate / store job.
2. Using the calendar, select the **Start Date** on which to execute the migrate / store job.
3. Click **Submit** to save the project. The project will run as scheduled.

While the job is active, hovering over the total bytes for the job in the Migrate / Store Jobs section of the Migrate / Store screen displays the migrate / store performance, see Figure 117 on page 230.

Set Recurring Schedule

If you select **Set Recurring Schedule**, the dialog box updates to display the following fields:

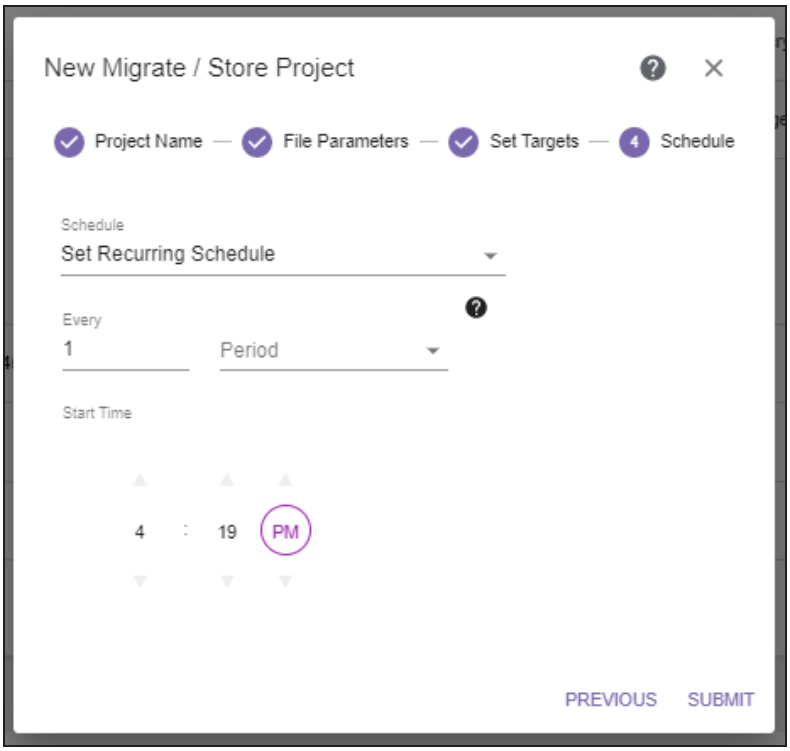


Figure 79 Setting a recurring schedule.

1. Select on what **Period** (daily, weekly, monthly) to execute the migrate store job.
   - If you selected **Daily**, continue with Step 2.
   - If you selected **Weekly**, select the day of the week on which to execute the migrate / store job and then continue with Step 2.
   - If you selected **Monthly**, select the day of the month on which to execute the migrate / store job. If you select a day of the month that is not valid for all months (for example, the 31st), the last day of the month is used in shorter months.
2. Specify the **Interval**, of days, weeks, or months, before the next migrate / store job executes. For example, if this value is set to 1, the job executes every day, week, or month, if the value is set to 2 the job executes every other day, week, or month, etc.
3. Use the up and down arrows to select the **Start Time** for executing the migrate / store job.
4. Click **Submit** to save the project. The project will run as scheduled.

While the job is active, hovering over the total bytes for the job in the Migrate / Store Jobs section of the Migrate / Store screen displays the migrate / store performance, see Figure 117 on page 230.

Run a Migrate / Store Project

To run a recurring or single-run Migrate / Store project, click **Actions > Run now** next to the project on the Migrate / Store screen (see Figure 73 on page 168). The Migrate / Store job runs immediately.

Pause a Migrate / Store Project

Pausing a migrate / store project stops a project with a recurring schedule, or a single run project scheduled for the future, from running. It does not remove the project from the list of projects on the Migrate / Store screen (see Figure 73 on page 168).

Note: Pausing a project does not cancel a job that is currently running. To cancel a migrate / store job that is queued, verifying, or active, see Cancel a Migrate / Store Job on the next page.

To pause a migrate / store project, click **Actions > Pause or Disable** next to the project that you want to pause. In the Pause / Disable window, select **Pause Project Schedule** from the Choose Action drop-down list, and click **Submit**.

To resume a paused project, see Resume a Migrate / Store Project below.

Resume a Migrate / Store Project

Resuming a migrate / store project restarts the schedule for a project with a recurring schedule or a single run project scheduled to run in the future.

Note: If the current time is past the scheduled run time for a single run project, the job does not run when resumed.

To resume a migrate / store project, click **Actions > Resume or Disable** next to the project that you want to resume (see Figure 73 on page 168). In the Resume / Disable, select **Resume Project Schedule** from the Choose Action drop-down list, and click **Submit**. The project will run at the next scheduled time.

CANCEL A MIGRATE / STORE JOB

To cancel a queued, verifying, or active migrate / store job, click **Actions > Cancel** next to the job on the Migrate / Store screen (see Figure 73 on page 168) or the Active and Completed Jobs screen (see Figure 116 on page 230). A confirmation screen displays. Click **Cancel Job** to confirm the cancellation.

The StorCycle solution leaves the data selected for transfer in the migrate / store job in whatever completion state it was in when the job cancellation command was received. No rollback occurs. For example, if some, but not all files were already transferred, they are not removed from the target. If all files were transferred and the source file replacement was started before the job was canceled, the source files are not replaced in the source directory.

IMPORTANT If you cancel a migrate / store job that uses a BlackPearl system as the target, and the final storage target of the BlackPearl data policy is offline or unavailable, the job stays in a "canceling" state until the final storage target is back online so that the data in process can persist to the final storage target.

Canceling a migrate / store job does not stop recurring migrate / store projects from running again. To stop a project with a recurring schedule from running again, see Disable a Migrate / Store Project.

VIEW MIGRATE / STORE JOB DETAILS

Click the name of the job to see the information entered when creating or editing the Migrate / Store project.

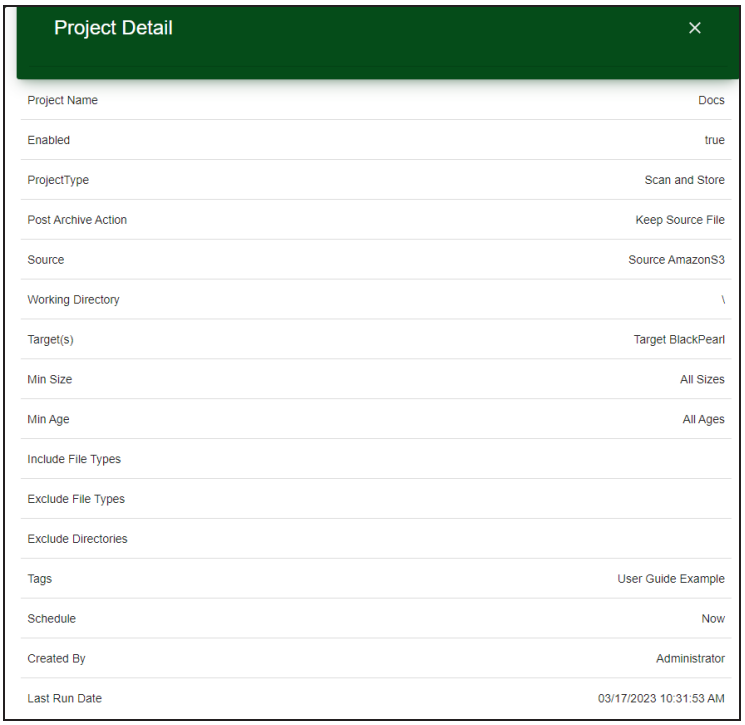


Figure 80 Migrate / Store project details.

EDIT A MIGRATE / STORE PROJECT

To edit a migrate / store project, click **Actions > Edit** next to the project that you want to edit (see Figure 73 on page 168).

Any field in a migrate / store project can be edited except the **Project Name**, **Source**, or whether to scan before migrate / store operations, or to use the last scan. See Create a Migrate / Store Project on page 166 for field descriptions.

Notes:
- Changing the **Schedule** for a recurring project to **Run Now** runs the job immediately.
- Editing a project with a **Schedule** currently set to **Run Now** does not run the job immediately. Click **Actions > Run Now** to run the job.
- You can change the target of a migrate / store job from a non-encrypted storage location to an encrypted storage location, but you cannot change the target from an encrypted storage location to a unencrypted storage location.
- You cannot mix encrypted targets and unencrypted targets in a single migrate / store project.

Clone a Migrate / Store Project

To clone a migrate / store project, click **Actions > Clone** next to the project on the Migrate / Store screen (see Figure 73 on page 168). The screen of the Migrate / Store wizard displays a project with the name Clone - *original Migrate / Store project name* and with the settings from the original migrate / store project entered.

Note: The default schedule for a cloned project is **Start Now**.

Cloning a Migrate / Store project does not clone data previously migrated by the project.

Update the Migrate / Store wizard fields as desired. See Migrate / Store Wizard—Project Name on page 169 for instructions.

Disable a Migrate / Store Project

Disabling a migrate / store project stops a project with a recurring schedule, or a single run project scheduled for the future, from running and removes it from the list of projects on the Migrate / Store screen (see Figure 73 on page 168).

Note: Disabling a project does not cancel a job that is currently running. To cancel a migrate / store job that is queued, verifying, or active, see Cancel a Migrate / Store Job on page 181.

Disabling a project does not delete the catalogs that were created based on that project. Use the search functionality in the StorCycle solution Restore wizard to retrieve files.

To disable a migrate / store project, do one of the following:

- For a single run project, click **Actions > Disable** next to the project on the Migrate / Store screen (see Figure 73 on page 168). A confirmation screen displays. Click **Disable** to confirm disabling the project.
- For a Recurring project, click **Actions > Pause or Disable** or **Actions > Resume or Disable**, select **Disable Project** from the **Choose Action** drop-down list. A confirmation screen displays. Click **Disable** to confirm disabling the project.

  Note: Even after disabling the project, the project name cannot be reused.

DELETE PROJECT

Use the instructions below to delete all files associated with a migrate / store project.

Note: The **Delete Project** link is only available for Administrator or Crypto Officer users.

1. Click **Delete Project** in the taskbar. The Delete Project screen displays.

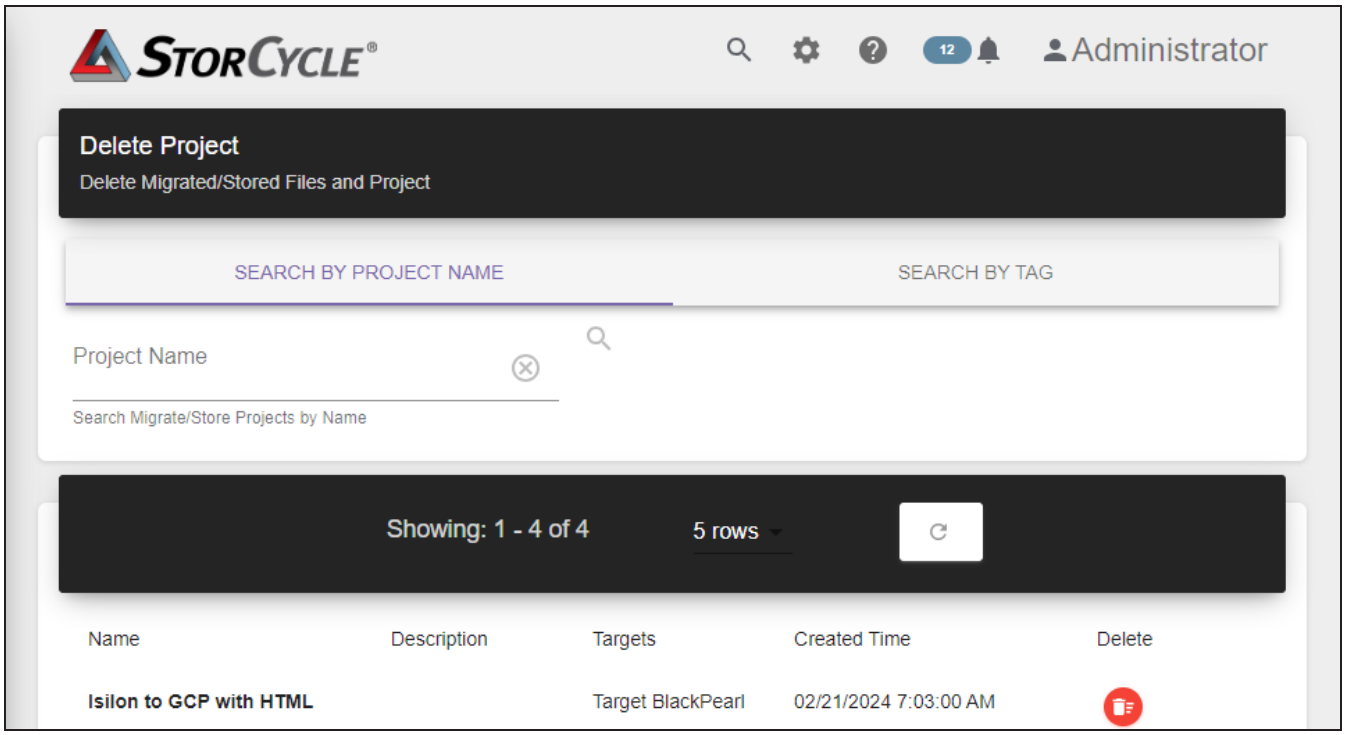


Figure 81 The Delete Project screen.

2. Select how you want to search.
   - **Search by Project Name on the next page**
   - **Search by Tag on page 186**

Search by Project Name

1. Project Names are displayed at the bottom of the screen. To filter the project names, enter the full or partial name in the **Project Name** field and click **Search**. The screen refreshes displaying matching projects.

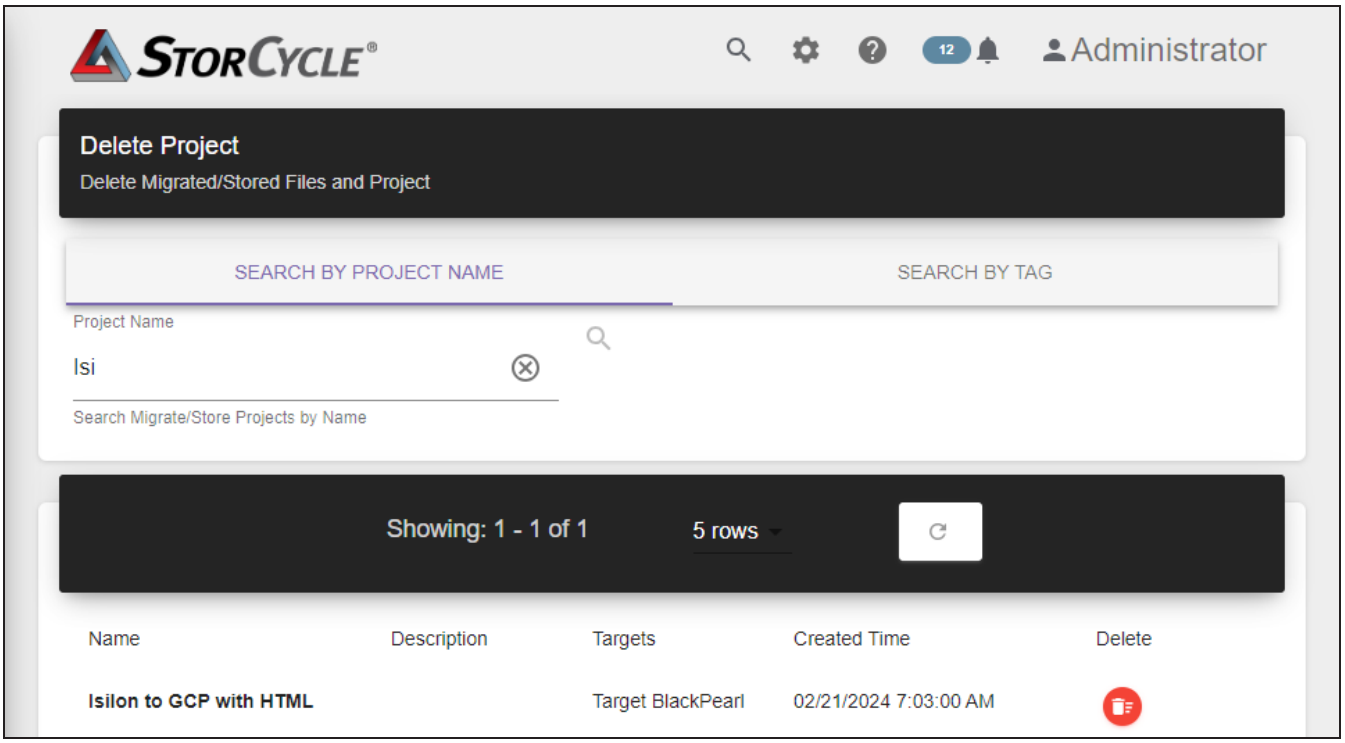


Figure 82 The Delete Project screen with matching projects.

2. Click **Delete** next to the project which migrated / stored the files you want to delete.
3. Type `Delete Objects` and click **Delete** to delete all project files from all storage targets.

CAUTION Once you type `Delete Objects` and click **Delete**, you cannot recover the files from the targets.

Search by Tag

1. Enter the full or partial tag you want to search for in the **Tag** field and click **Search**. The screen refreshes displaying matching projects.

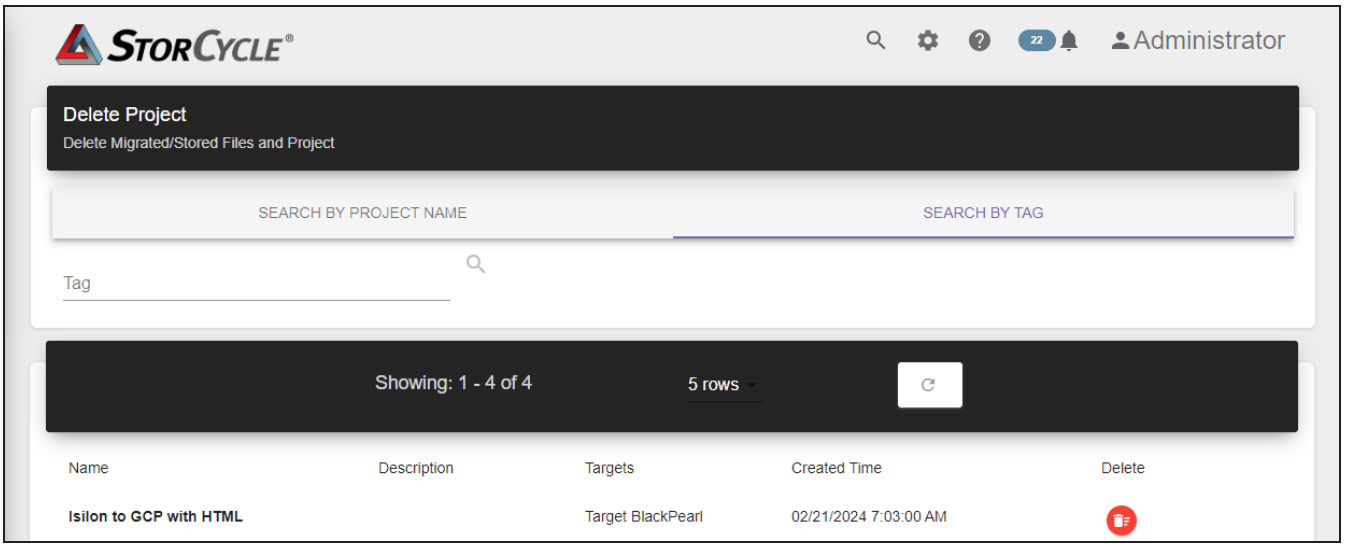


Figure 83 Searching by Tag on the Delete Project screen.

2. Click **Delete** next to the project which migrated / stored the files you want to delete.
3. Type `Delete Objects` and click **Delete** to delete all project files from all storage targets.

CAUTION Once you type `Delete Objects` and click **Delete**, you cannot recover the files from the targets.

Chapter 10 - Restore and Browse Objects

This section provides instructions for using the Restore wizard and Browse Objects page.

Notes:
- For highest performance, when restoring an object that was migrated / stored to multiple types of targets, the StorCycle solution attempts to restore the object from NAS storage first, then a BlackPearl system, and finally cloud storage.
- When more than 10 jobs are running on the StorCycle solution, restore jobs are prioritized at the top of the job queue.

RESTORE USING HTML LINKS

If you selected **Remove Source File: create HTML link** or **Remove Source Files: replace with single HTML link** as the **Replacement Option** when you created the migrate / store project (see Step 2 on page 175), you can open the HTML file present in the original file location for shortcuts to restore an individual file or all files that were migrated / stored in the same project.

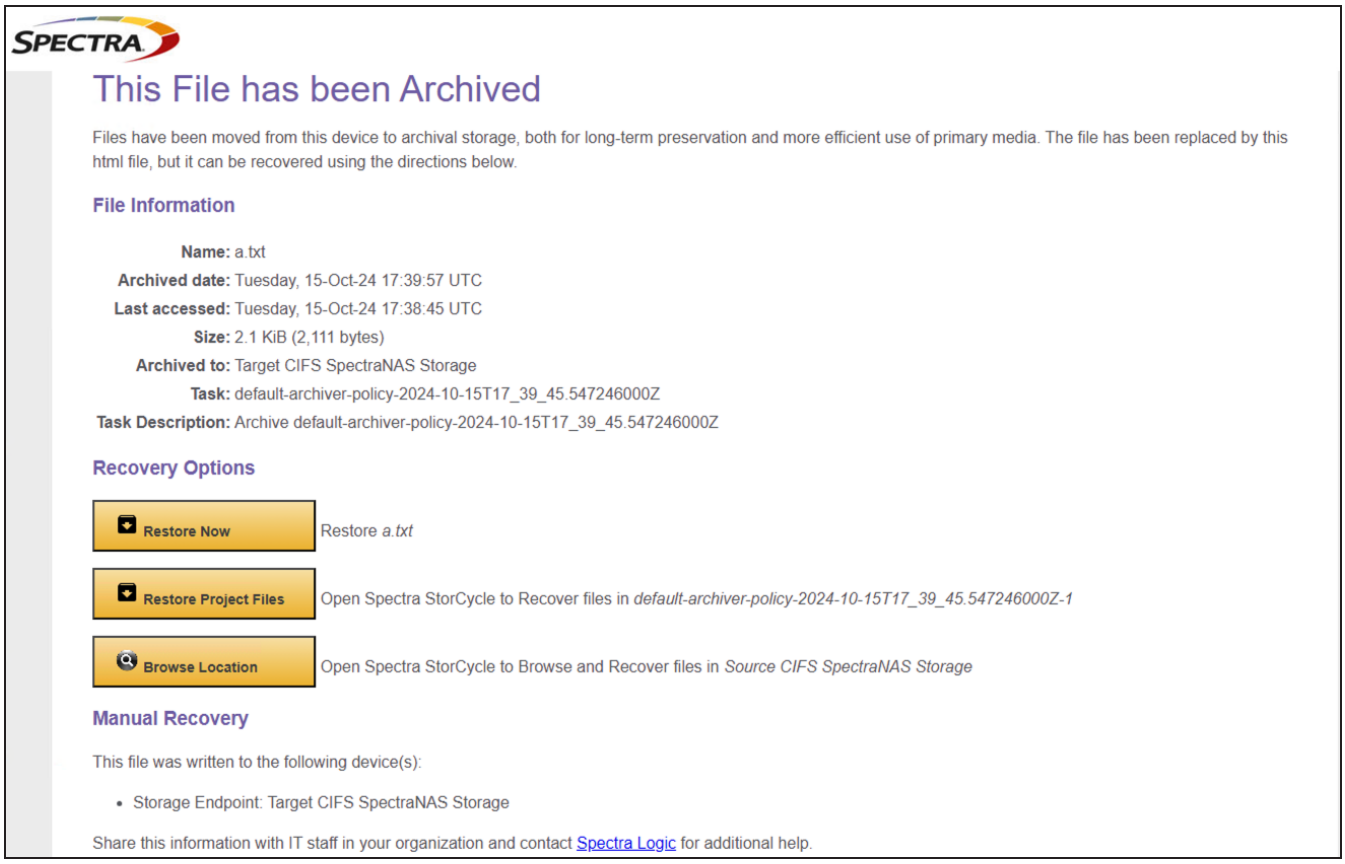


Figure 84 An HTML link for a stored file.

Click **Restore Now** to restore the individual file, **Restore Project Files** to restore all files in the migrate / store project, or **Browse Location** to view all files in the storage location. The Spectra StorCycle Solution login screen displays.

Note: If an SSL Certificate has not been added to the StorCycle solution, you may get a warning from the browser that the site is not secure.

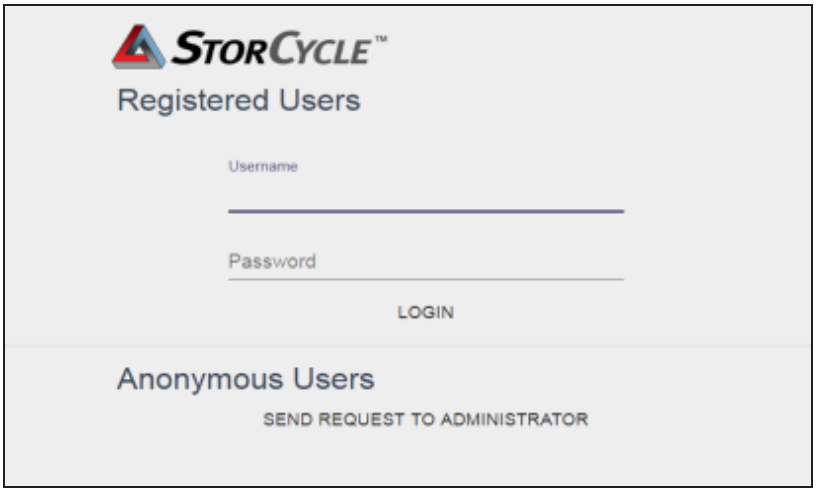


Figure 85 The Spectra StorCycle Solution Login screen with link to email the Administrator.

If you are a registered user, log in to complete the restore. The Restore wizard runs with all fields populated to restore the requested file(s). See Restore Wizard—Files to Restore on page 192 for more information.

If Active Directory / LDAP was configured with **Allow any Active Directory / LDAP user to restore** selected (see Configure Active Directory / LDAP on page 137), any Active Directory / LDAP user on the domain can restore files even if they are not configured as a StorCycle user. Log in using your Active Directory credentials.

If Active Directory / LDAP was not configured or not configured with **Allow any Active Directory / LDAP user to restore** selected, and you are not a registered user, click **Send Request to Administrator**. The Send Request to Administrator screen displays.

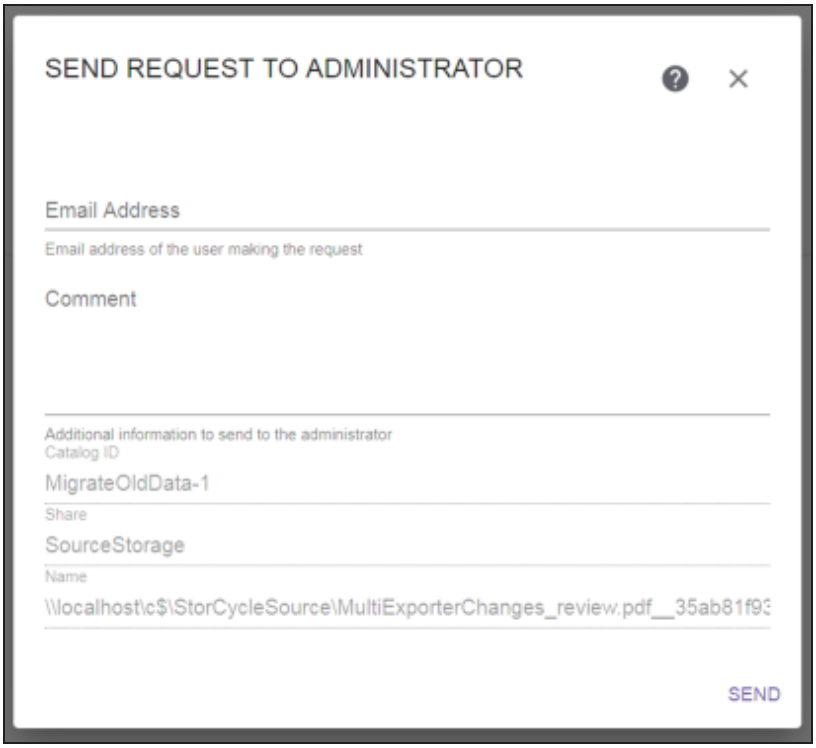


Figure 86 The Send Request to Administrator screen.

Enter your **Email Address** and, if desired, a **Comment**, and then click **Send** to email the request to the Spectra StorCycle solution Administrator.

Note: To use this form, SMTP must be configured (see Configure SMTP on page 147) and an email address must be configured for the Administrator user (see Edit a User on page 146).

Restore Using Symbolic Links

If you selected **Remove Source File: create Symbolic link** as the **Replacement Option** when you created the Migrate / Store Project (see Step 2 on page 175), in most cases you can transparently open the replaced files from secondary storage by double-clicking the file name.

In some cases, double-clicking a symbolic link generates an error indicating that the file cannot be opened. If this happens, try launching the program associated with the file and opening the file with the program.

IMPORTANT Files opened using symbolic links are read-only. If you want to edit the file, you need to save it with a different name on your primary storage.

CREATE A RESTORE PROJECT

Configure a restore project to move data from secondary storage back to primary storage.

Use the instructions below to configure a new restore project.

1. Click **Restore** in the taskbar. The Restore screen displays showing configured restore projects and current and completed restore jobs.

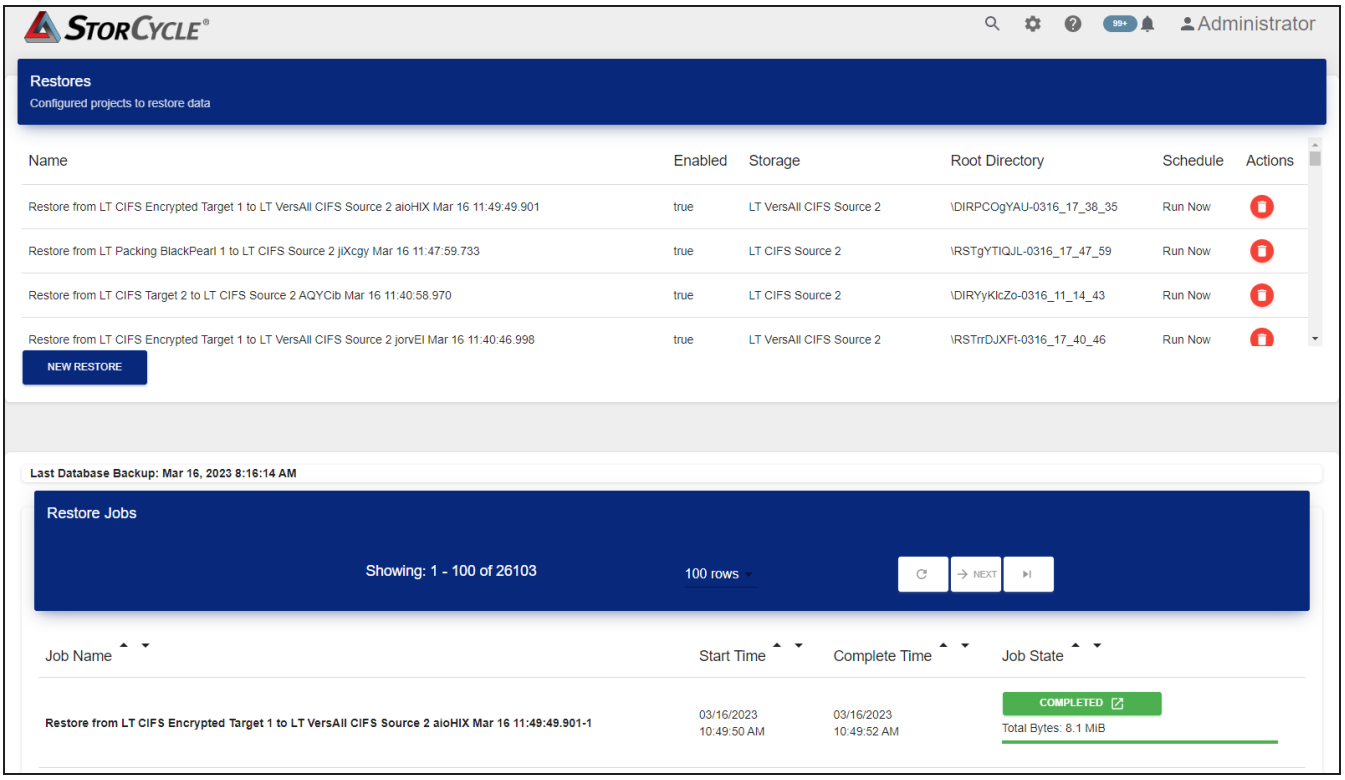


Figure 87 The Restore screen.

2. Click **New Restore** to start the Restore wizard.

Restore Wizard—Files to Restore

The Files to Restore screen of the Restore wizard allows you to select from which migrate / store project to restore files.

IMPORTANT If storage locations use storage location security, The restore wizard will only display projects associated with source storage locations configured with an AD / LDAP group to which you are a member. See Storage Location Security on page 84 for more information.

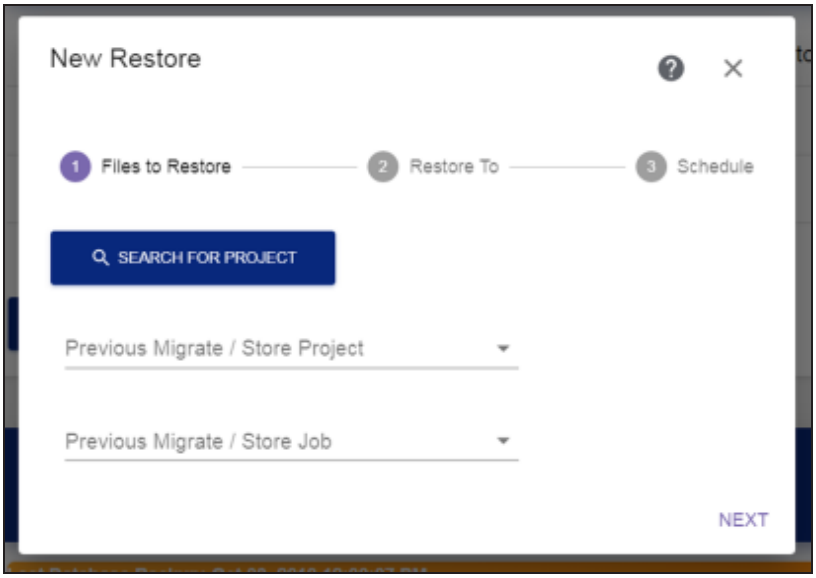


Figure 88 The Files to Restore screen of the Restore wizard.

- Click **Search for Project** to open the Catalog Search Dialog box (see Search for Project on the next page for instructions).
- Use the drop down fields to Select the Project Manually (see Select the Project Manually on page 197 for instructions).

Search for Project

The Catalog Search dialog box allows you to search for a project.

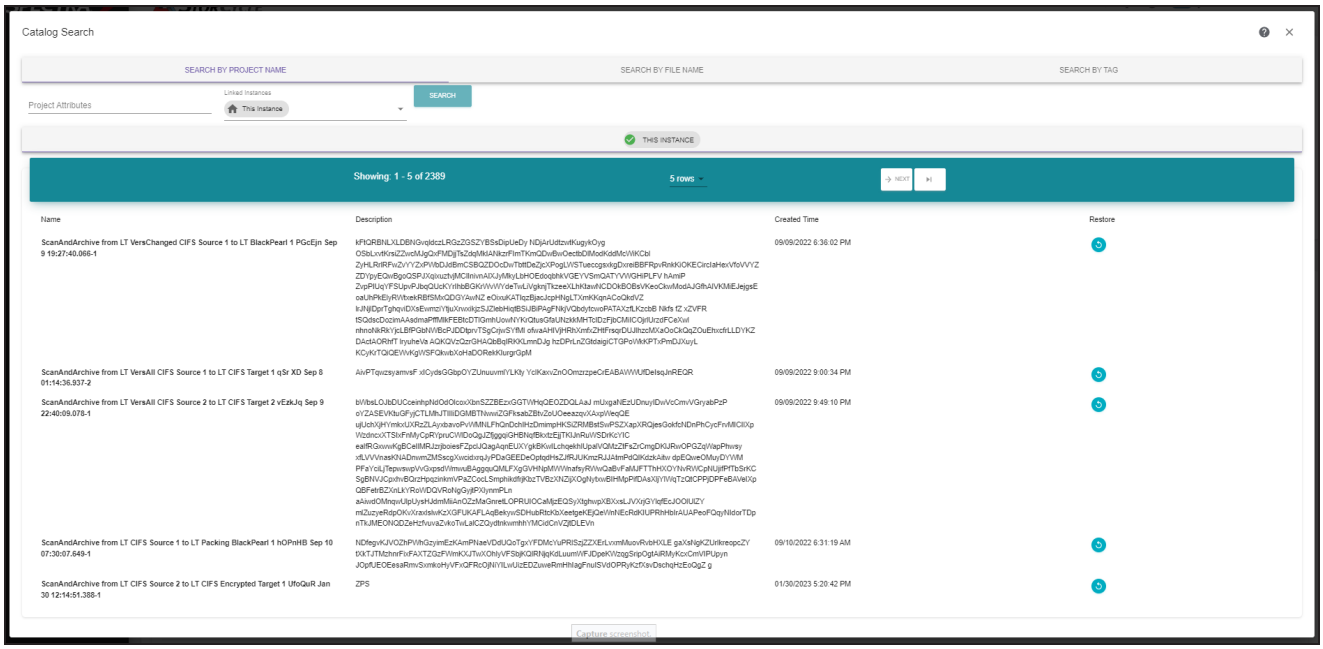


Figure 89 The Search by Project Name tab of the Catalog Search dialog box.

Select the tab indicating how you want to search:

- Search by Project Name on the next page
- Search by File Name on page 195
- Search by Tag on page 197

Search by Project Name

1. If applicable, select which StorCycle instances you want to search. The default is this instance only. See Configure Linked Instances on page 215 for information on configuring linked instances.
2. In the **Project Attributes** field, enter the full or partial project name or description, and click **Search**.

   The tab for each linked instance included in the search displays the number of matches found. Select a tab to see all migrate / store jobs executed by a project with a name or description containing the search string.
3. Click **Restore** next to the job from which you want to restore files.
4. The user interface returns to the Restore wizard with the correct **Previous Migrate / Store Project** and **Previous Migrate / Store Job** selected.

Note: If the job is on a linked instance, you will need to log into the linked StorCycle solution and continue creating the restore project on that instance. Files can only be restored to storage locations configured in the linked instance.

5. Continue with Select Files to Restore on page 198.

Search by File Name

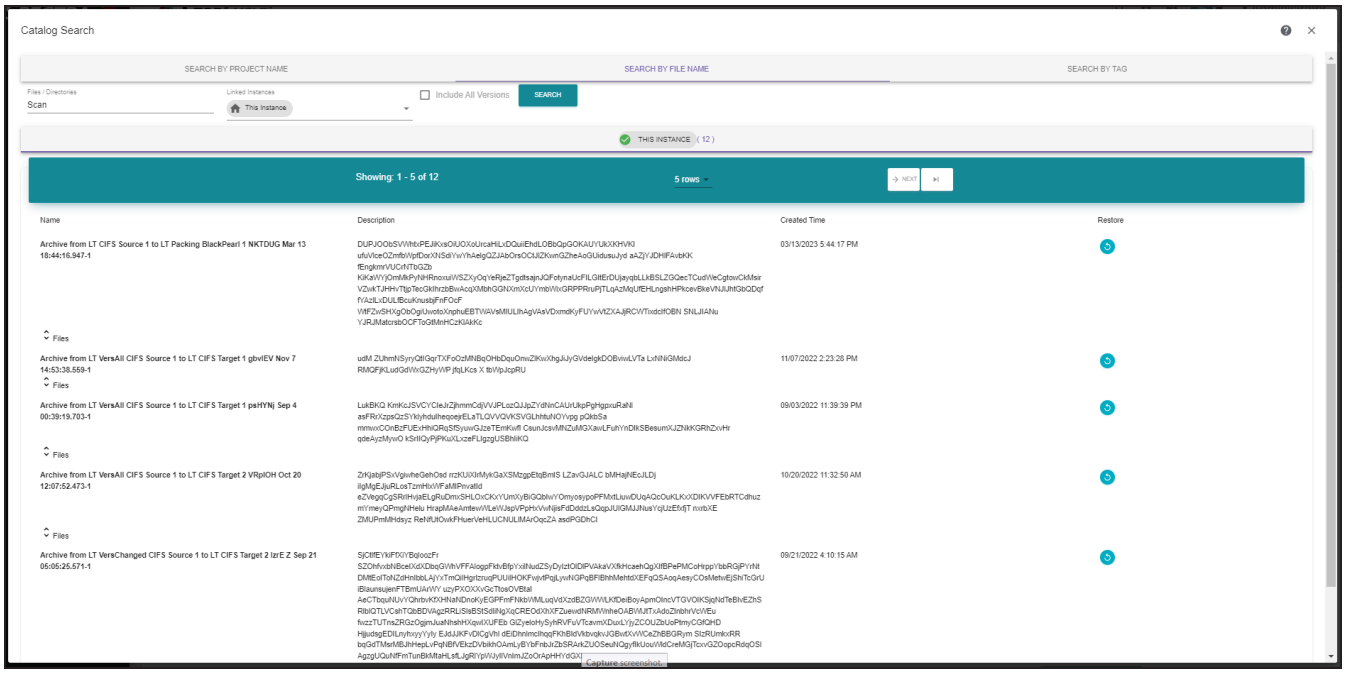


Figure 90 The Search by File Name tab of the Catalog Search dialog box.

1. If applicable, select which StorCycle instances you want to search. The default is this instance only. See Configure Linked Instances on page 215 for information on configuring linked instances.
2. If applicable, select whether to **Include All Versions**. See Versioning on page 83 for information on versioned sources.

Note: This setting can be toggled after searching for files.

3. In the **Files / Directories** field, enter the full or partial file or directory name, and click **Search**.

   If you selected one or more linked instances, a tab for each linked instance included in the search displays the number of matches found.

   If you selected **Include All Versions**, the screen displays a **Latest Version** tab and a **Versioned Files** tab for this instance of StorCycle software. The **Latest Version** tab displays the latest version of all files. The **Versioned Files** tab displays all versions of versioned files including the latest version with a code appended to the file name that indicates the date and time that the file was migrated / stored in the format `yyyymmddhhmmss` using a 24-hour clock.

   Select a tab to display all migrate / store jobs containing a file or directory with a name containing the search string.

Notes:
- Non-versioned files do not display on the **Versioned Files** tab.
- Linked Instances only display the latest version of files.
- When a versioned file is restored, the data and time information is removed from the file name.
- If a job is restored from a target with packing enabled and which contains a versioned file which has been deleted due to **keep XX versions**, the StorCycle solution does not include the deleted file in the restore, even if it still exists in a pack. The deleted version does not exist in the StorCycle database and the restore job completes without warnings or errors.

4. Click **Restore** next to the job from which you want to restore files. Alternatively, expand the project and select a single file to restore.
5. The user interface returns to the Restore wizard with the correct **Previous Migrate / Store Project** and **Previous Migrate / Store Job** selected. Or, if you selected a single file, the information for the single file is automatically populated.

Note: If the job is on a linked instance, you will need to log into the linked StorCycle solution and continue creating the restore project on that instance. Files can only be restored to storage locations configured in the linked instance.

6. Continue with Select Files to Restore on page 198.

Search by Tag

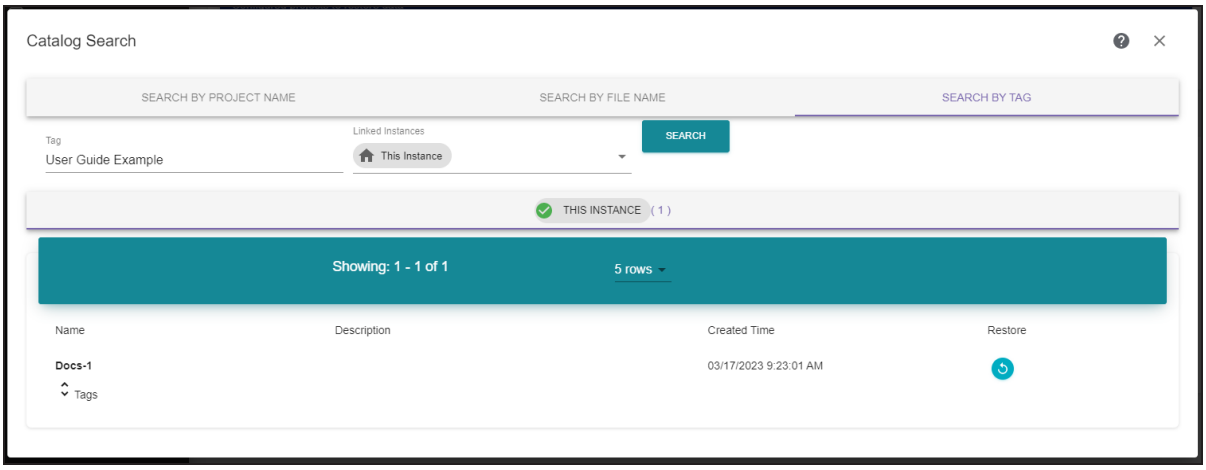


Figure 91 The Search by Tag tab of the Catalog Search dialog box.

1. If applicable, select which StorCycle instances you want to search. The default is this instance only. See Configure Linked Instances on page 215 for information on configuring linked instances.
2. In the **Tag** field, enter a full or partial tag, and click **Search**.

   The tab for each linked instance included in the search displays the number of matches found. Select a tab to see all migrate / store jobs with a tag containing the search string.
3. Click **Restore** next to the job from which you want to restore files.
4. The user interface returns to the Restore wizard with the correct **Previous Migrate / Store Project** and **Previous Migrate / Store Job** selected.

Note: If the job is on a linked instance, you will need to log into the linked StorCycle solution and continue creating the restore project on that instance. Files can only be restored to storage locations configured in the linked instance.

5. Continue with Select Files to Restore on the next page.

Select the Project Manually

1. From the **Previous Migrate / Store Project** drop-down, select a previously configured project which executed the job from which you want to restore files. See Migrate or Store Data on page 164.
2. From the **Previous Migrate / Store Job** drop-down, select the previously executed job from which you want to restore files.

Note: If the project was deleted manually or because of retention policy, the drop-down for **Previous Migrate / Store Job** will be empty.

3. Continue with Select Files to Restore on the next page.

Select Files to Restore

Select **Restore All Files in Project**, **Specify Single File**, or **Browse File Listing**.

Depending on which option you select, the dialog box updates to display more fields. Continue with the applicable section below:

- Restore All Files in Project
- Specify Single File
- Browse File Listing

Restore All Files in Project

If you select **Restore All Files in Project**, all files in the migrate / store job are restored. Click **Next** and continue with Restore Wizard—Restore To on page 200.

Specify Single File

If you select **Specify Single File**, the dialog box updates to request the file name.

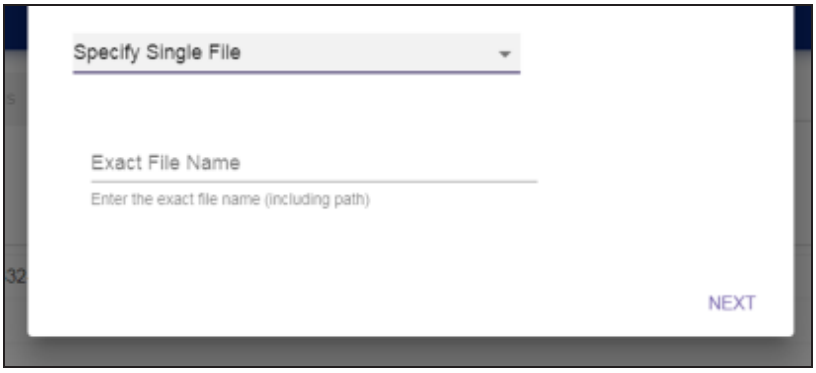


Figure 92 The Specify Single File restore fields.

1. In the **Exact File Name** field, enter the full file name including the path to the share and the file extension.
2. Click **Next** and continue with Restore Wizard—Restore To on page 200.

Browse File Listing

If you select **Browse File Listing**, the dialog box updates to display all files and sub-directories in the selected job.

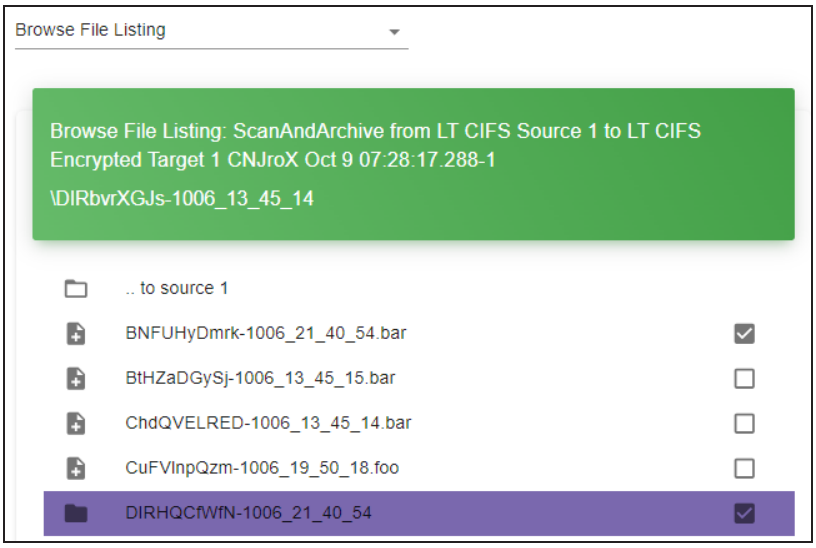


Figure 93 The Browse File Listing restore fields.

1. Browse to find the files or directories that you want to restore and select the check box next to the name. Directories highlight purple when selected.
2. Click **Next** and continue with Restore Wizard—Restore To on the next page.

Restore Wizard—Restore To

The Restore To screen of the Restore wizard allows you to configure the location where the objects will be restored.

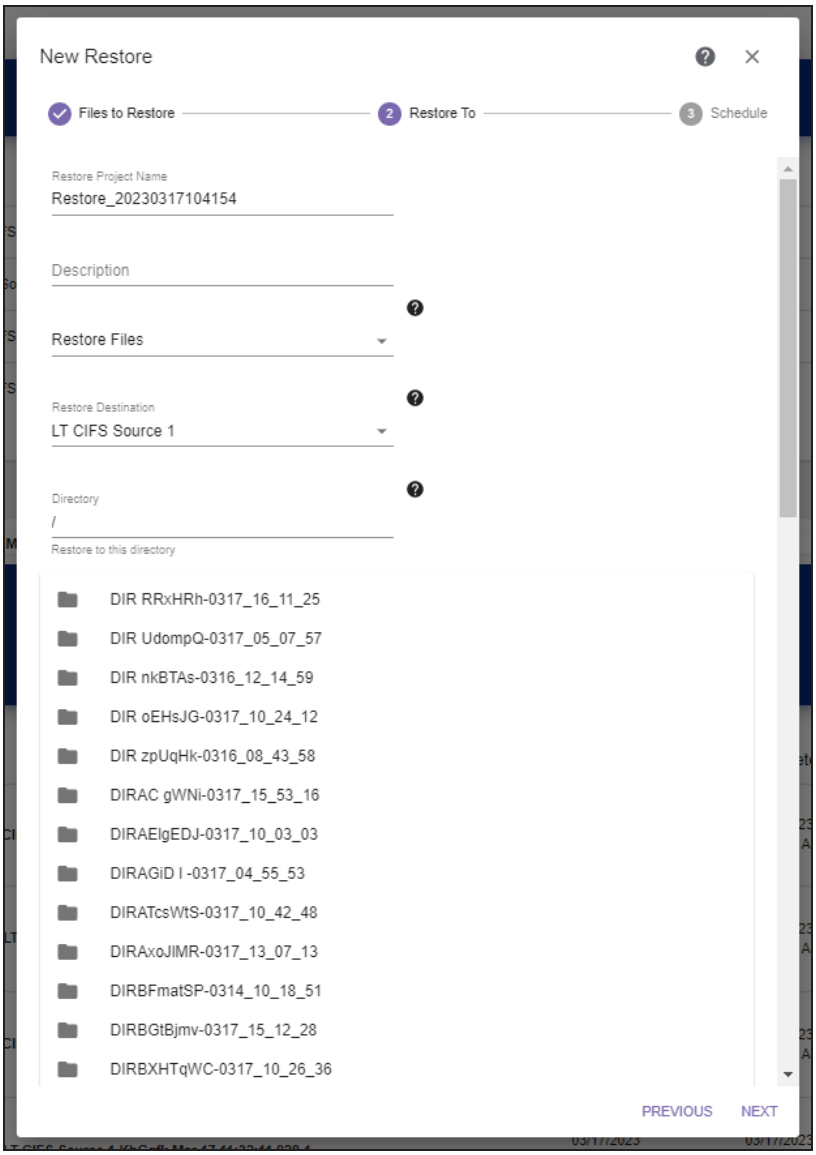


Figure 94 The Restore To screen of the Restore wizard.

1. If desired, edit the **Restore Project Name**.

IMPORTANT A project name must be unique across all scan, migrate / store, restore, and database backup projects. Names of deleted projects cannot be reused.

2. If desired, enter a project **Description**.
3. Select whether to **Restore Files**, **Restore Individual HTML Links**, **Restore Single HTML Link**, or **Restore Symbolic Links Only**.
   - **Restore Files** —The file is restored to restore destination.
   - **Restore Individual HTML Links**—An HTML link to instructions for restoring the file from secondary storage is placed in the restore destination.
   - **Restore Symbolic Links**—A symbolic link to the file on a NAS target is placed in the restore destination.

   Note: The **Restore Symbolic Links Only** option is only available if the original migrate / store project used the **Create Symbolic Links** option.
4. If you are restoring Symbolic links, the original source location is entered as the Restore Destination. Symbolic links can only be restored to the source location of the original migrate / store job. Continue with Restore Wizard—Schedule.

   If you are restoring files or HTML links, from the **Restore Destination** drop-down, select one of the following:

   - Select **Create New Source** and enter the **Storage Location Name** and **Server Path** for a new NAS storage location

   Note: If you want to add additional detail for the new storage location, see Edit a Storage Location on page 125.

IMPORTANT

Storage location server paths should not overlap. For example:

- The storage location server path should not be a sub-directory of an existing storage location path.
- The storage location server path should not have a sub-directory that is used by an existing storage location path.
- The storage location server path cannot be the same as an existing storage location path with different capitalization.

IMPORTANT The server path name should not be the same as a BlackPearl bucket that you plan to ingest. See Ingest Data in BlackPearl Bucket on page 123 for more information.

- Select one or more previously configured storage location(s) as the destination. The directory structure of the **Restore Destination** displays.

5. Select the starting sub-directory on the **Restore Destination** to be the restore directory.

IMPORTANT If you restore to a location other than the original source location, the StorCycle solution attempts to restore the original permissions of each file, but may not be able to depending on the properties of the restore location.

Notes:

- If a restore project attempts to restore a file to a location in which a file of the same name already exists, the restore fails. The existing file is not overwritten.
- If symbolic links were created for migrated files, when the files are restored to their original location, the symbolic links are deleted.
- If HTML links were created for migrated files, when the files are restored to their original location, the HTML links are deleted or retained depending on Remove HTML Links on Restore setting on the Global Settings screen. See "Configure Global Settings" on page 135.
- On Windows system files and CIFS file shares, the StorCycle solution migrate / stores and restores file permissions / ACLs, but does not migrate / store Alternative Data Streams or SACLs.
- When the StorCycle solution migrates / stores or restores files, it also migrates / stores or restores associated directories. While the StorCycle solution ensures that a file does not already exist on the target and does not overwrite the file, it may overwrite existing directories.
  - When the Windows version of the StorCycle solution overwrites a directory, it resets the permissions / ACLs based on the permissions / ACLs that are on the directory that it is migrating.
  - When the Linux version of the StorCycle solution overwrites a directory, it does not reset the permissions / ACLs (because Linux does not have an "Auto Inherit" flag like Windows).
- Spectra Logic recommends that you restore files to a new directory location.
- Having the target directory for a migrate / store job open in Windows Explorer may cause "The process cannot access the file because it is being used by another process" errors.
- If files were migrated / stored from an S3 source to a BlackPearl storage location they can only be restored to a Spectra or Non-Spectra NAS storage location and metadata is not restored.

Restore Wizard—Schedule

The Schedule screen of the Restore wizard allows you to configure when to run the restore project.

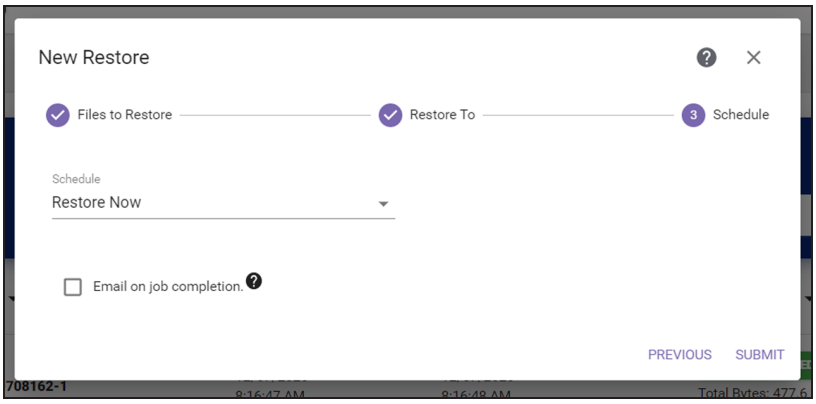


Figure 95 The Schedule screen of the Restore wizard.

Select **Restore Now** or **Set Restore Time** to set the run schedule.

- Restore Now below
- Set Restore Time on the next page

Restore Now

1. If desired, select the **Email on job completion** check box to have an email sent to the logged in user when the restore completes.
2. Click **Submit** to save the project. The project starts immediately.

   While the job is active, hovering over the total bytes for the job in the Restore Jobs section of the Restore screen displays the restore performance, see Figure 117 on page 230.

Set Restore Time

If you select **Set Restore Time**, the dialog box updates to display the following fields:

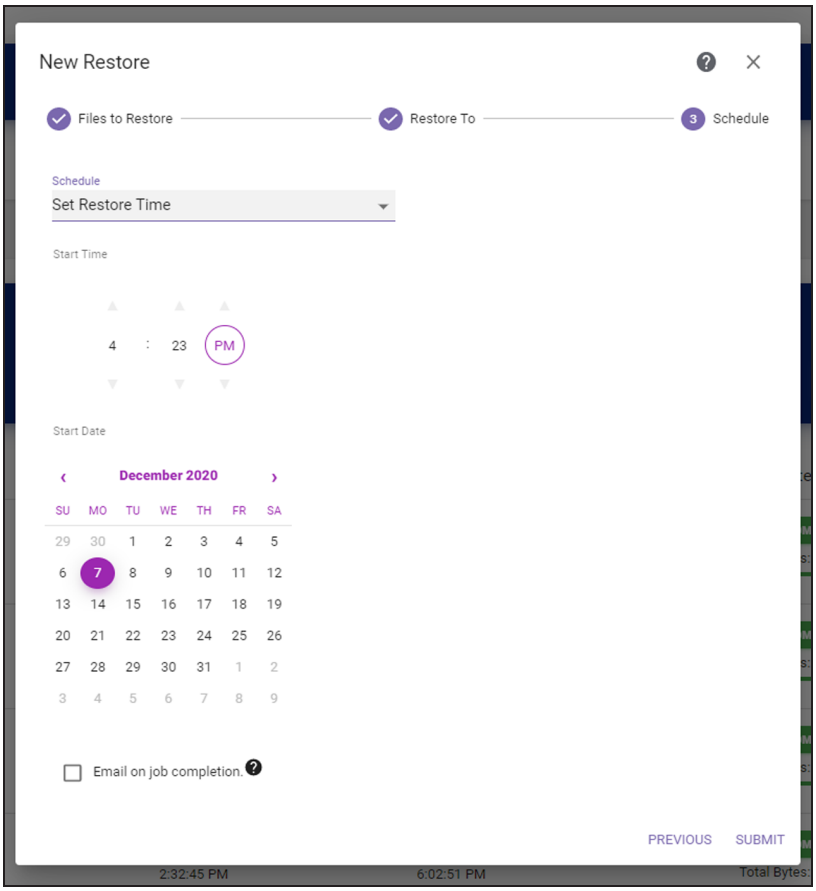


Figure 96 Setting a start time.

1. Use the up and down arrows to select the **Start Time** for executing the restore.
2. Using the calendar, select the **Start Date** on which to execute the restore.
3. If desired, select the **Email on job completion** check box to have an email sent to the logged in user when the restore completes.
4. Click **Submit** to save the project. The project runs as scheduled.

   While the job is active, hovering over the total bytes for the job in the Restore Jobs section of the Restore screen displays the scan performance, see Figure 117 on page 230.

CREATE A RESTORE PROJECT USING BROWSE OBJECTS

Configure a restore project to move data from secondary storage back to primary storage by searching for and selecting all desired data.

Use the instructions below to configure a new restore project using browse objects by source.

1. Click **Browse** on the taskbar. The Browse Objects screen displays.

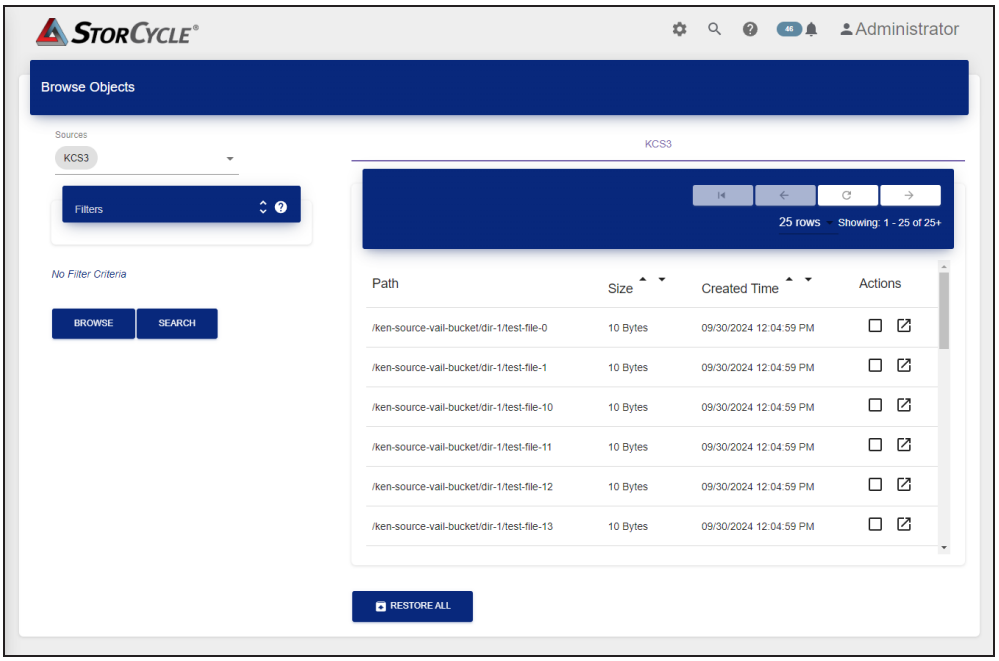


Figure 97 The Browse Objects screen.

2. Using the **Sources** drop-down menu, select an existing project to browse / search.

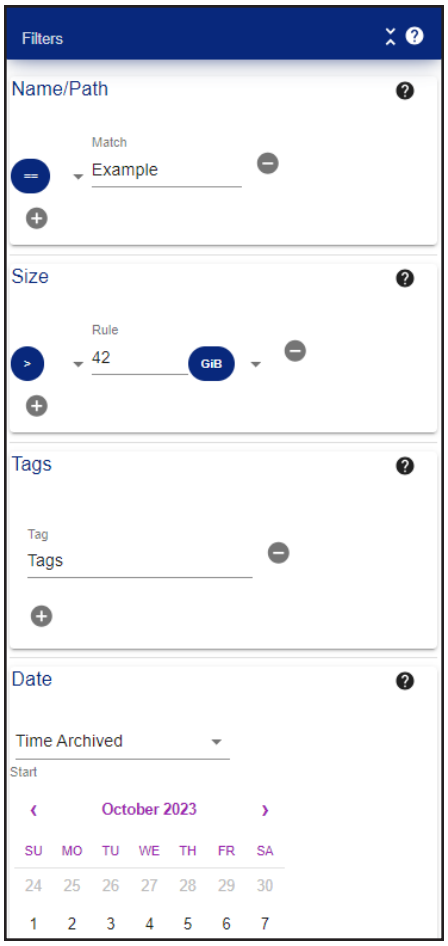


Figure 98 The Filters option windows.

3. If desired, apply filters to the search. Click **Filters** to expand the filter options. The following filters are supported:

- **Name/Path**—The Name/Path filter searches for files in the specified directory or files with matching names. The Name/Path filter supports a set of additional search operation parameters accessible through a drop-down menu: **==** (equals), **!=** (not equal), **^_** (starts with), **_$** (ends with), and ***_*** (contains).
- **Size**—The Size filter searches for files in a specified size or range. Use the left drop-down menu to apply **<** (less than), **>** (greater than), **==** (equals), and **!=** (not equal) operations. Use the right drop-down menu to select B, KiB, MiB, GiB, and TiB units.
- **Tags**—The Tags filter searches for files with exact tag matches.
- **Date**—The Date filter searches for files in a specified date range. From the drop-down menu, select between **Time Archived**, **Last Accessed Time**, **Creation Time**, or **Last Modified Time** then select a start date from the calendar display below.

Note: You can click the **+** button in the bottom left to add an additional filter in the **Name/Path**, **Size**, and **Tags** categories.

4. Select either **Browse** or **Search** to run the search.

Note: The **Search** button executes a full search across all directories. This operation may take a long period of time and cannot be canceled.

5. After the search completes, select the check box under **Actions** (see Figure 97 on page 205) to add the file to the restore list.

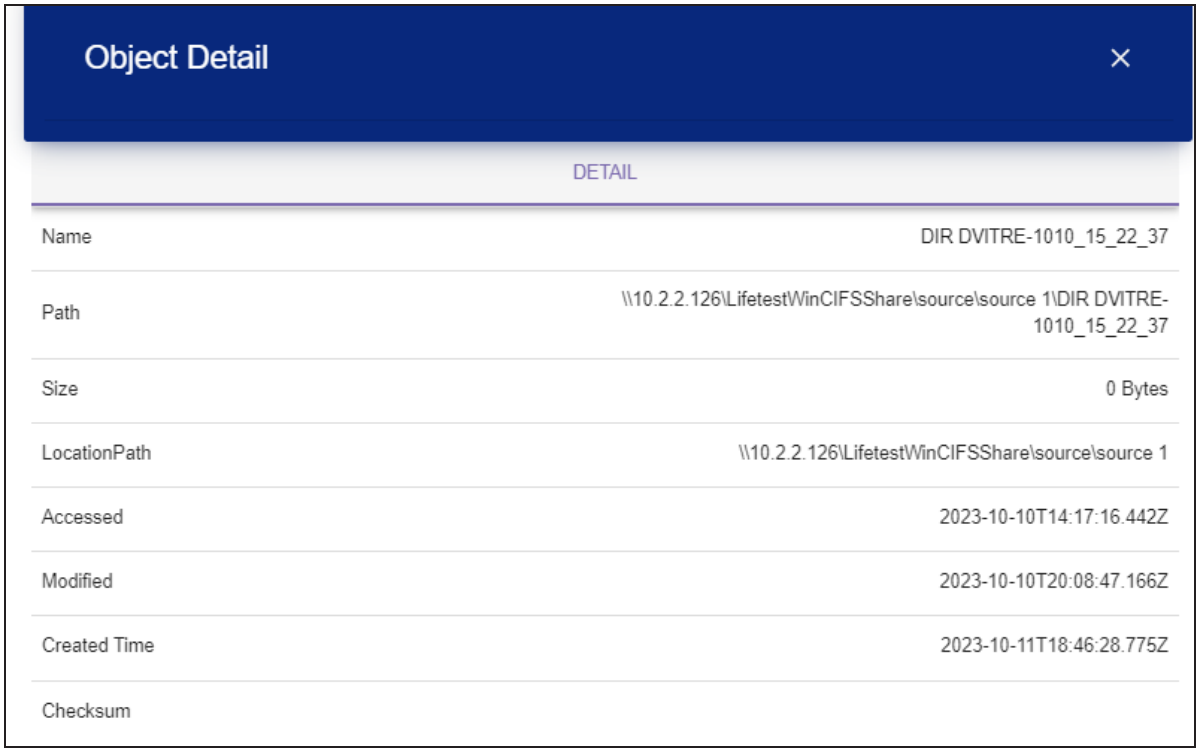


Figure 99 The Object Detail screen.

6. Optionally, click the **Job Details** icon to view the **Name**, **Path**, **Size**, **LocationPath**, **Accessed**, **Modified**, **Created Time**, and **Checksum** information.

7. Click the **Restore Selected** to restore all selected objects. If no objects are selected, the **Restore All** displays. Click the **Restore All** to restore all browse results.

Cancel a Restore Job

To cancel a queued, verifying, or active restore job, click **Cancel** next to the job on the Restore screen (see Figure 87 on page 191) or the Active and Completed Jobs screen (see Figure 116 on page 230). A confirmation screen displays. Click **Cancel Job** to confirm the cancellation. The StorCycle solution leaves the data being transferred by the restore job in whatever completion state it was in when the job cancellation command was received. No rollback occurs.

Disable a Restore Project

Disabling a restore project removes it from the list of projects on the Restore screen (see Figure 87 on page 191). To disable a restore project, click **Disable** next to the project on the Restore screen. A confirmation screen displays. Click **Delete** to confirm disabling the project.

Note: Even after disabling the project, the project name cannot be reused.

Accessing Migrated / Stored Files Without the Spectra StorCycle Solution

Files migrated / stored by the Spectra StorCycle solution are typically accessed by using symbolic links, HTML links, or the StorCycle solution to restore the files to a source storage location. However, users can also access the files directly on the target storage without using the StorCycle solution.

IMPORTANT If a file is changed on the target after being migrated / stored, attempting to restore the file using the StorCycle solution fails.

The StorCycle solution writes files to storage targets using the original file names and directory structures, except when using packs on a BlackPearl system. Pack object names include the Job Name and UUID.

When the storage target is a BlackPearl system and tape, the tapes are written in the open LTFS format, which means that the tapes can be read by the Spectra Eon browser or any other system that supports LTFS. Use a BlackPearl data policy that uses object naming mode so the BlackPearl system uses the actual file names on the LTFS tape.

Chapter 10 - Other Settings and Features

This section provides instructions for configuring non-required settings that help you use the StorCycle solution.

ENABLE ENCRYPTION

The StorCycle solution supports a single encryption key for all storage targets. The key used for encryption and decryption is saved in memory. If the server reboots, the encryption password must be re-entered. The StorCycle solution automatically regenerates the encryption key.

CAUTION Safely store the encryption password in a secure location. If you lose the encryption password, you are not able to use the StorCycle solution to restore the encrypted data after a server reboot. Additionally, any migrate / store jobs to an encrypted target fail.

IMPORTANT Once encryption is enabled and the encryption password is set, it cannot be disabled and the password cannot be changed.

IMPORTANT StorCycle encryption does not protect the file name and metadata information on the target.

IMPORTANT Only users with a Crypto Officer role can enable or disable encryption. See Configure Users on page 142 for more information about different user types.

Note: Using encryption may have a performance impact on the server CPU.

Use the following instructions to set an encryption password.

1. Click **Settings** in the toolbar and then select **Encryption**. The Encryption screen displays.

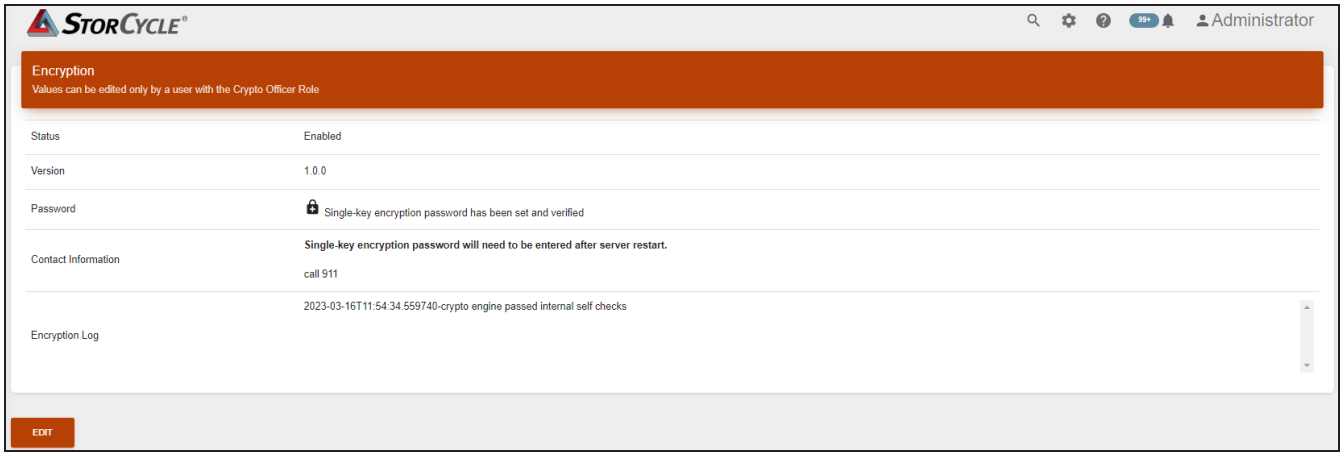


Figure 100 The Encryption screen.

2. Click **Set Password**. The Encryption dialogue box displays.

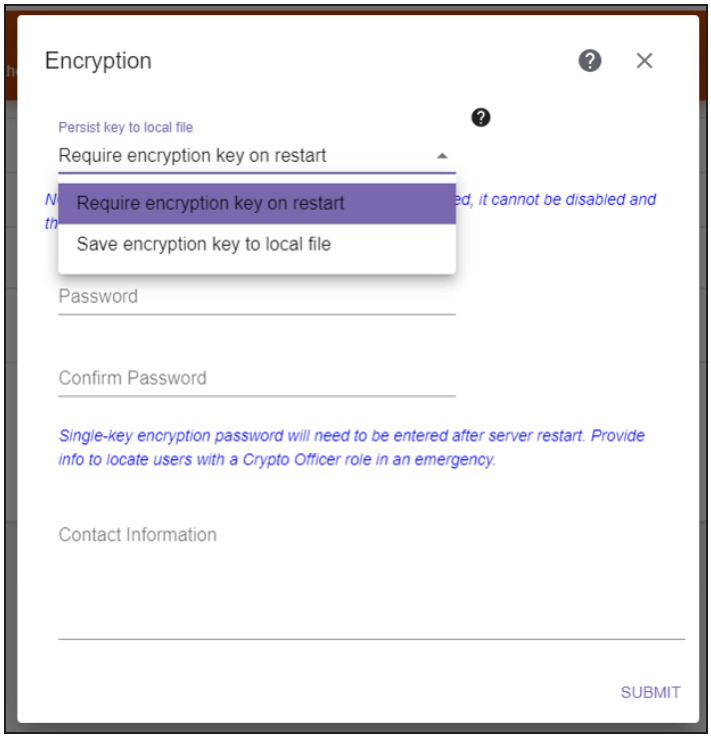


Figure 101 The Encryption dialog box.

3. Select either **Require encryption key on restart** or **Save encryption key to local file**.
4. Enter and confirm the **Password**.
5. Enter **Contact Information** for one or more Crypto Officers who can be contacted if the encryption password must be re-entered. You cannot enable encryption without providing contact information for a Crypto Officer.

IMPORTANT It is important to have up to date Crypto Officer contact information because migrate / store jobs to encrypted targets or restores from encrypted targets fail until the encryption password is re-entered after a StorCycle server reboot.

6. Click **Submit**.
7. Securely store the encryption password.

CAUTION If you lose the encryption password, you are not able to access the data stored by the StorCycle solution after a server reboot.

After enabling encryption and setting the encryption password, you can configure new storage locations to use encryption. See Configuring Storage on page 89 for more information.

Re-Enter the Encryption Password

A red banner displaying "Encryption password not set" indicates that the StorCycle server rebooted and you must re-enter the encryption password.

IMPORTANT Once encryption is enabled and the encryption password is set, it cannot be disabled and the password cannot be changed.

IMPORTANT Only users with a Crypto Officer role can re-enter the encryption password. See Configure Users on page 142 for more information about different user types.

Use the following instructions to re-enter the encryption password.

1. Click **Settings** in the toolbar and then select **Encryption**. The Encryption screen displays.

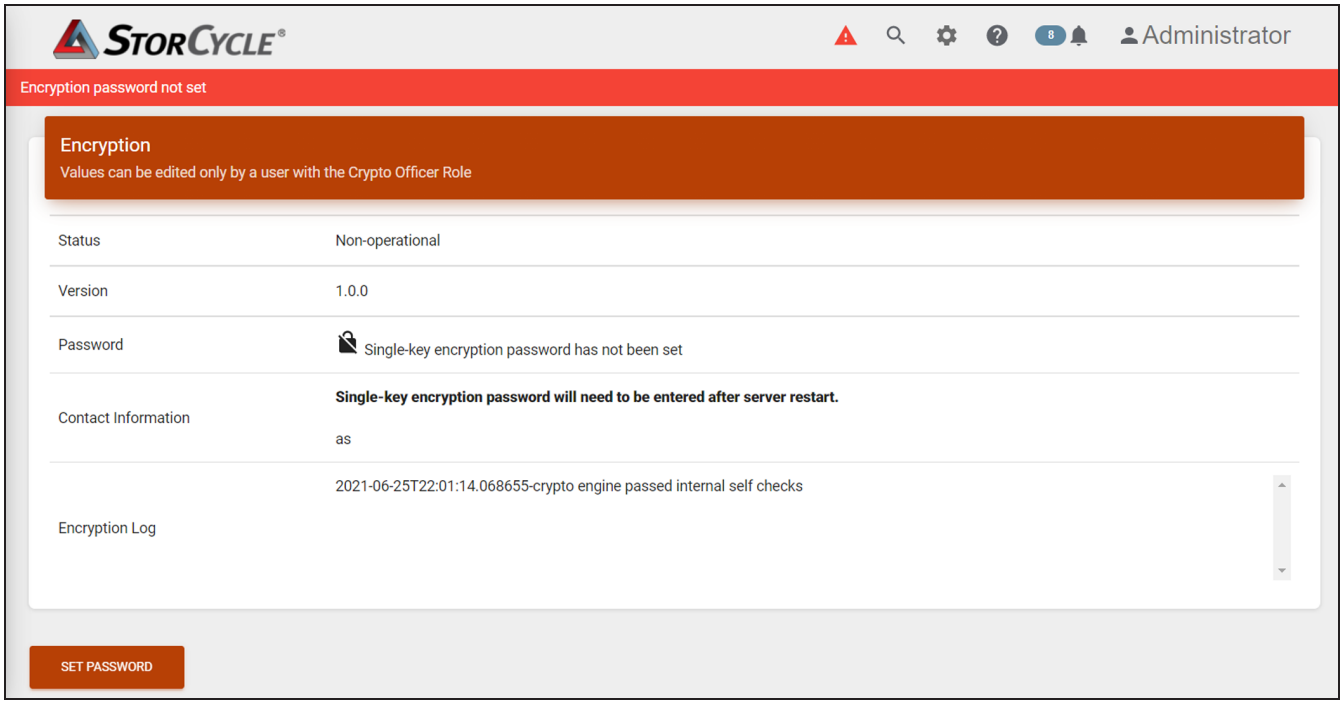


Figure 102 The Encryption screen.

2. Click **Set Password**. The Encryption dialogue box displays.

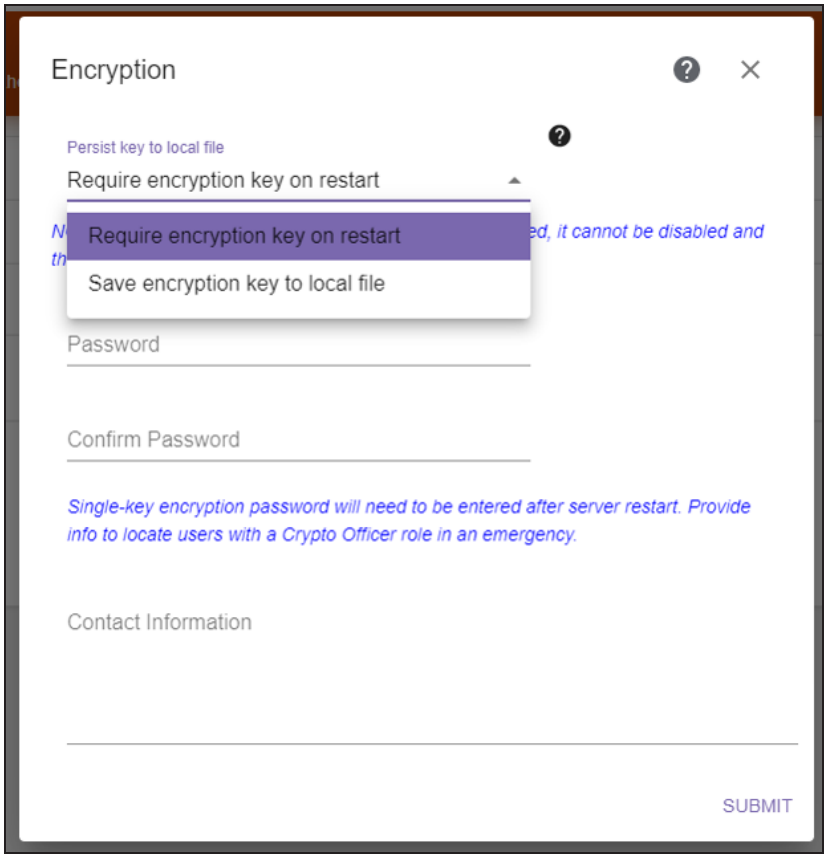


Figure 103 The Encryption dialog box.

3. Select either **Require encryption key on restart** or **Save encryption key to local file**.
4. Enter the **Password**.
5. Update the **Contact Information**.

IMPORTANT It is important to have up to date Crypto Officer contact information because migrate / store jobs to encrypted targets or restores from encrypted targets fail until the encryption password is re-entered after a StorCycle server reboot.

6. Click **Submit**.

After the password is submitted, the StorCycle solution regenerates the encryption key.

Edit Crypto Officer Contact Information

Use the following instructions to edit Crypto Officer contact information.

1. Click **Settings** in the toolbar and then select **Encryption**. The Encryption screen displays.

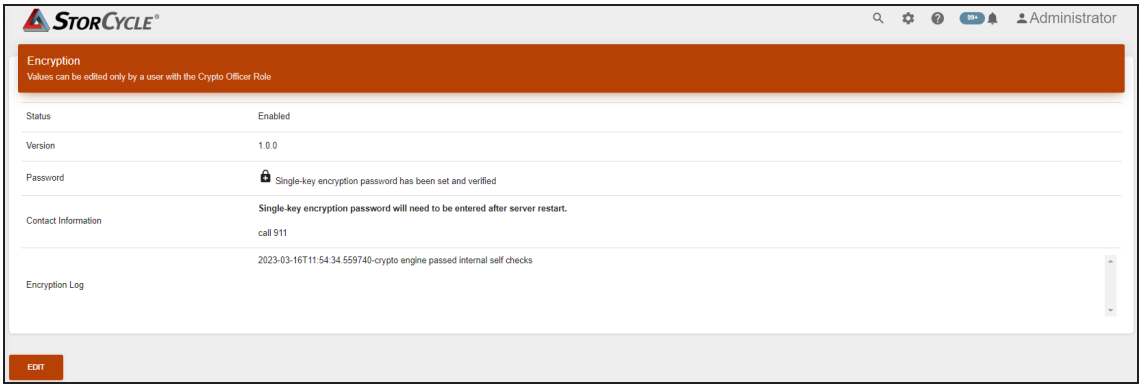


Figure 104 The Encryption screen.

2. Click **Edit** . The Encryption dialog box displays.

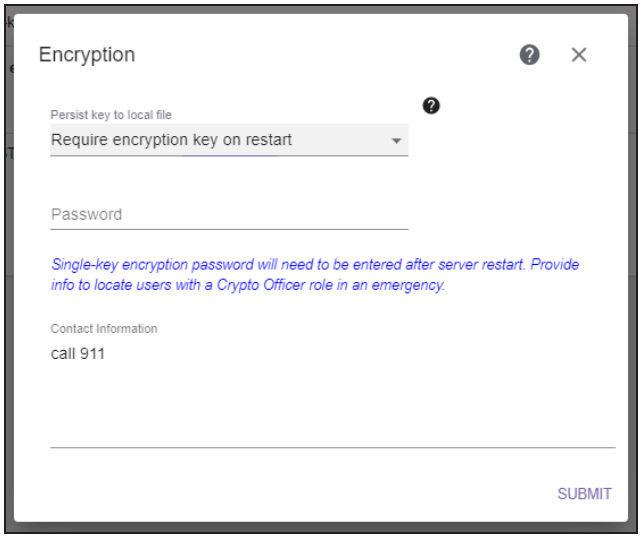


Figure 105 The Encryption dialog box.

3. Enter contact information for one or more Crypto Officers who can be contacted if the encryption password must be re-entered. You cannot enable encryption without providing contact information for a Crypto Officer.

IMPORTANT It is important to have up to date Crypto Officer contact information because migrate / store jobs to encrypted targets or restores from encrypted targets fail until the encryption password is re-entered after a StorCycle server reboot.

4. Click **Submit**.

CONFIGURE LINKED INSTANCES

Configure linked instances to search for data managed by other StorCycle solution installations. Linked instances are helpful when you have multiple StorCycle solutions installed and want to be able to use one instance to scan for data on the other instance.

The linked instance can be on the same server platform (Windows or Linux) or a different platform.

Note: All StorCycle instances must be at StorCycle version 3.5.0 or later, to be linked.

Use the instructions below to configure a linked instance.

1. Click **Settings** in the toolbar and then select **Linked Instances**. The Linked Instances screen displays showing all currently configured linked instances.

   Note: Linked instances are not bi-directional. If you want StorCycle instance A and StorCycle instance B to be able to search the other's managed data, you need to create a linked instance from StorCycle instance A to StorCycle instance B and then another from StorCycle instance B to StorCycle instance A.

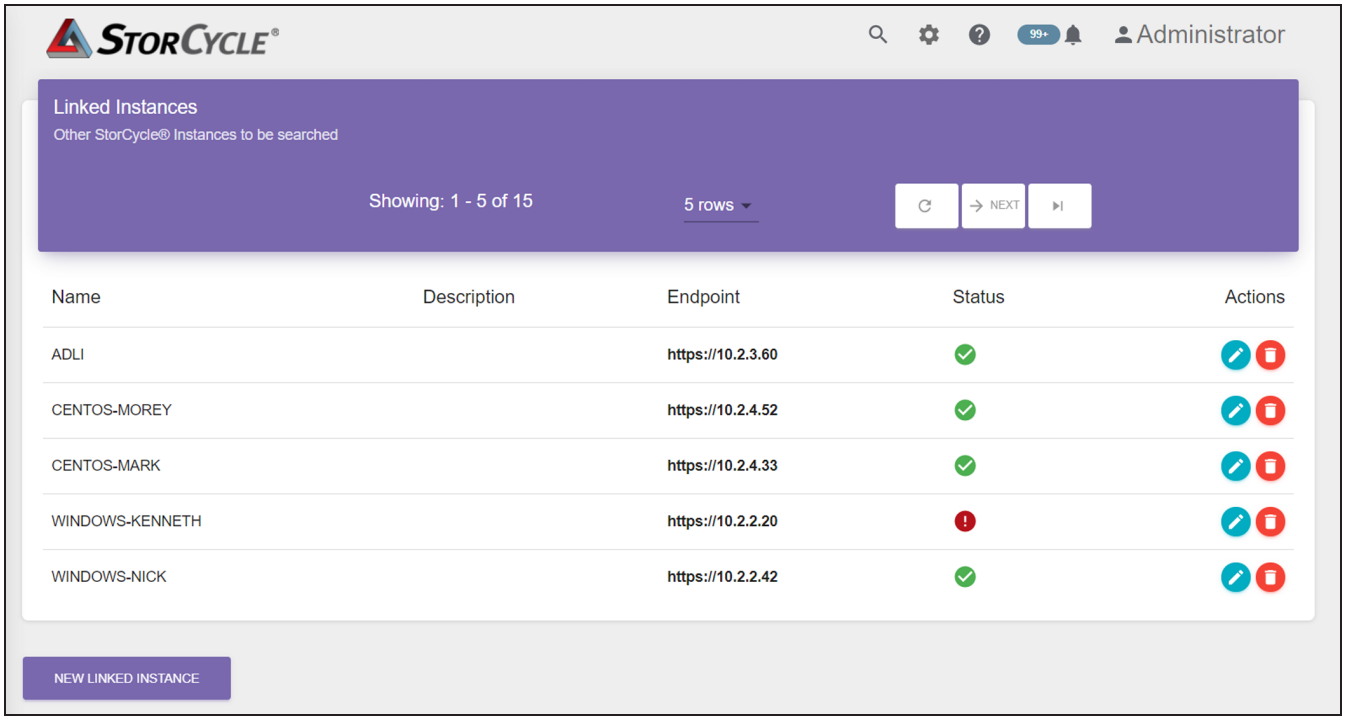


Figure 106 The Linked Instances screen.

2. Click **New Linked Instance**. The New Linked Instance dialog box displays.

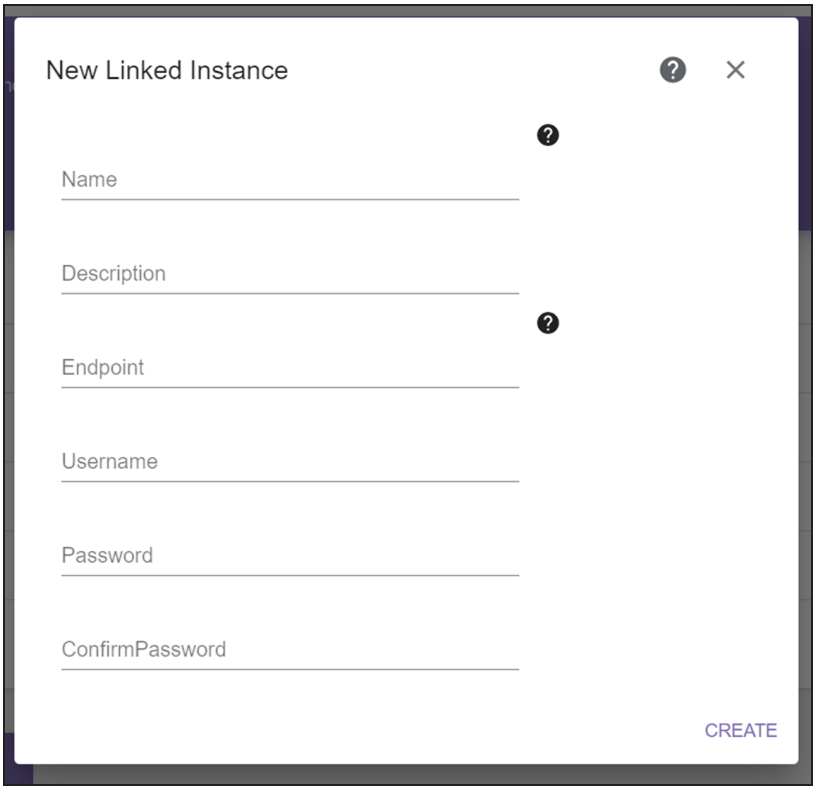


Figure 107 The New Linked Instance dialog box.

3. Enter a unique **Name** for the linked instance.
4. If desired, enter a **Description** for the linked instance.
5. Enter the **Endpoint** for the linked instance in the format `https:`*`xxx.xxx.xxx.xxx`*. Do not include `/app`. If the StorCycle instance does not use the default port, add *`:XXX`* to the endpoint, where *`XXX`* is the port number.
6. Enter the **Username** and enter and confirm the **Password** for a user configured on the StorCycle instance to which you are linking.
7. Click **Create** to configure the linked instance. The connection to the link instance is verified and the status displays on the Linked Instances screen.

Icon	Meaning	Description
	**Online**	The StorCycle solution successfully connected to the linked instance.
	**Unreachable**	The StorCycle solution could not connect to the linked instance. Hover over the icon for more information.

Edit a Linked Instance

To edit a linked instance, click **Edit** next to the linked instance on the Linked Instances screen (see Figure 106 on page 215). Edit the **Description**, **Username**, or **Password** as desired and click **Update**.

Delete a Linked Instance

To delete a linked instance, click **Delete** next to the linked instance on the Linked Instances screen (see Figure 106 on page 215). A confirmation screen displays. Click **Delete** to confirm the linked instance deletion.

REPLACE THE SSL CERTIFICATE

To view the currently installed SSL certificate, or access the screens to replace it, click **Settings** ⚙ in the toolbar and then select **Configuration > Licenses & SSL Certificate**. The Licenses & SSL Certificate screen displays showing all licenses and the SSL certificate currently installed in the software.

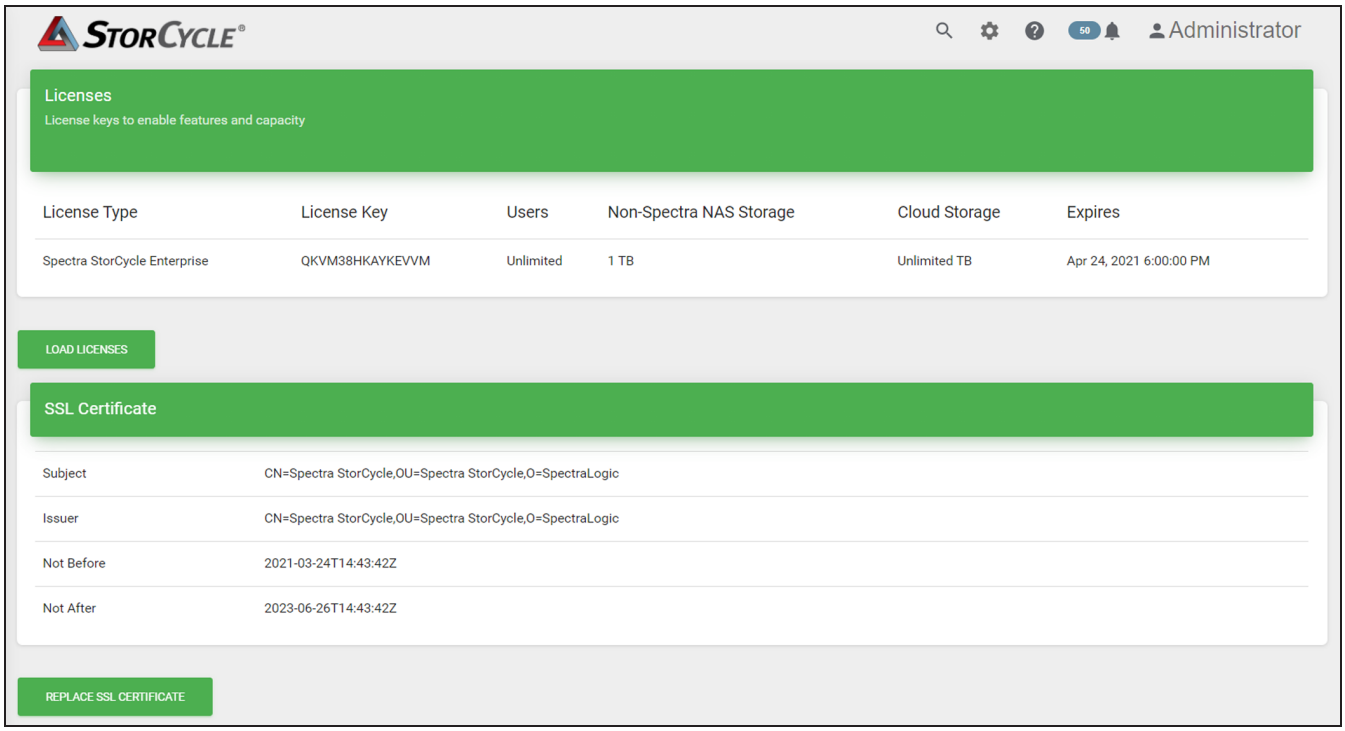


Figure 108 The Licenses & SSL Certificate screen.

Replace the SSL Certificate

The SSL certificate allows for signed security when using the StorCycle web interface. Use the instructions below to replace the SSL certificate.

1. Click **Replace SSL Certificate**. The SSL Certificate dialog box displays.

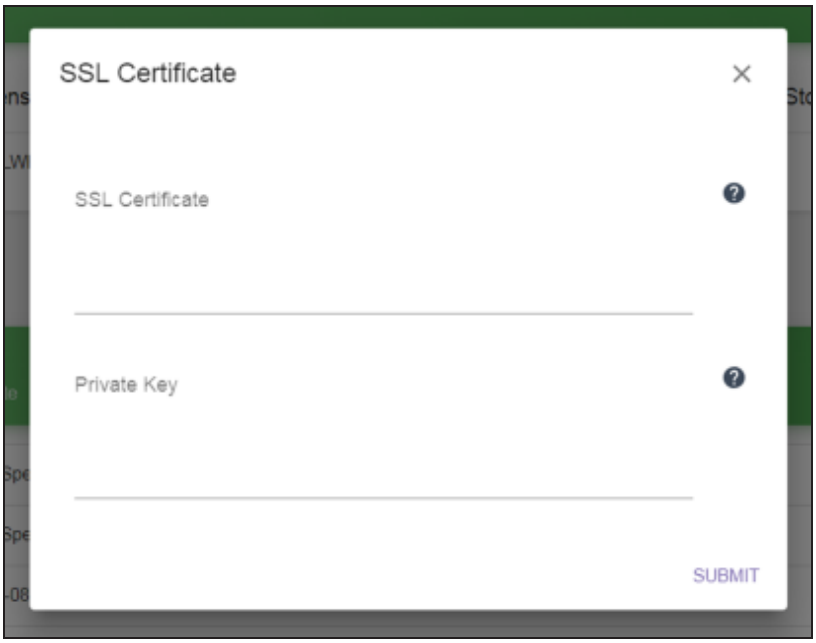


Figure 109 The SSL Certificate dialog box.

2. Copy and paste the **SSL Certificate** for the server, in PEM format.
3. Enter the **Private Key** that signed the SSL certificate, in PEM format.

CONFIGURE DEPARTMENTS

Configure departments to manage cost accounting by department.

Use the instructions below to configure a new department.

1. Click **Settings** in the toolbar and then select **Configuration > Departments**. The Departments screen displays showing all departments currently configured in the software.

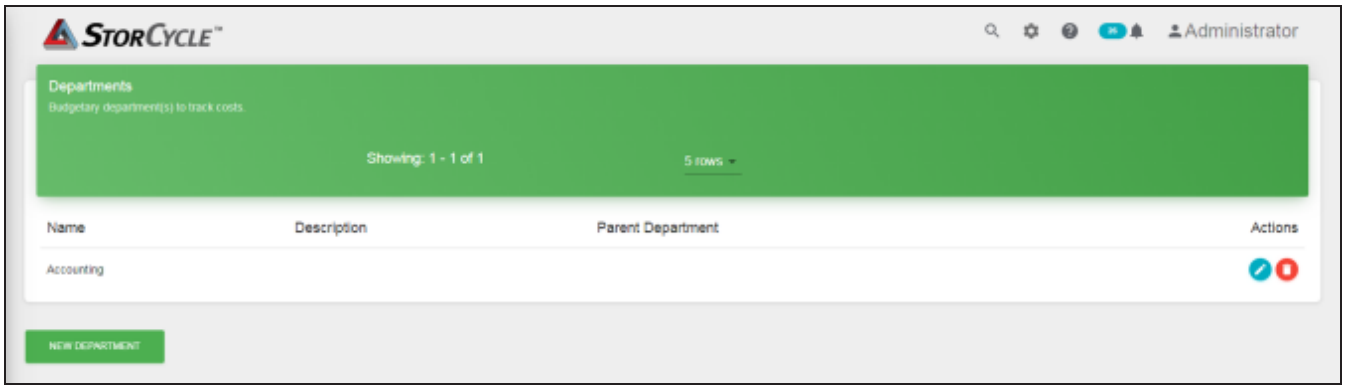


Figure 110 The Departments screen.

2. Click **New Department**. The New Department dialog box displays.

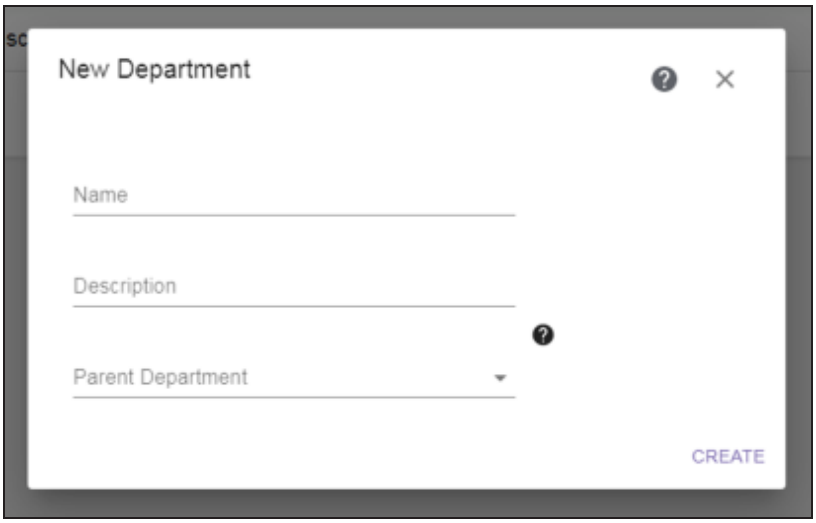


Figure 111 The New Department dialog box.

3. Enter a unique **Name** for the department.
4. If desired, enter a **Description** for the department.
5. If applicable, use the drop-down list to select the **Parent Department** to which this department belongs.
6. Click **Submit** to save the department configuration.

Edit a Department

To edit a department, click **Edit** next to the department on the Department screen (see Figure 110 on page 220). Edit the **Description** and **Parent Department** as desired and click **Update**. If you want to change the name of a department, delete the department and then recreate it with the new name.

Delete a Department

To delete a department, click the **Delete** next to the department on the Department screen (see Figure 110 on page 220). A confirmation screen displays. Click **Delete** to confirm the department deletion.

LOAD OR REMOVE LICENSES

To view the currently installed licenses, or access the screens to replace them, click **Settings** in the toolbar and then select **Configuration > Licenses & SSL Certificate**. The Licenses & SSL Certificate screen displays showing all licenses and the SSL certificate currently installed in the software.

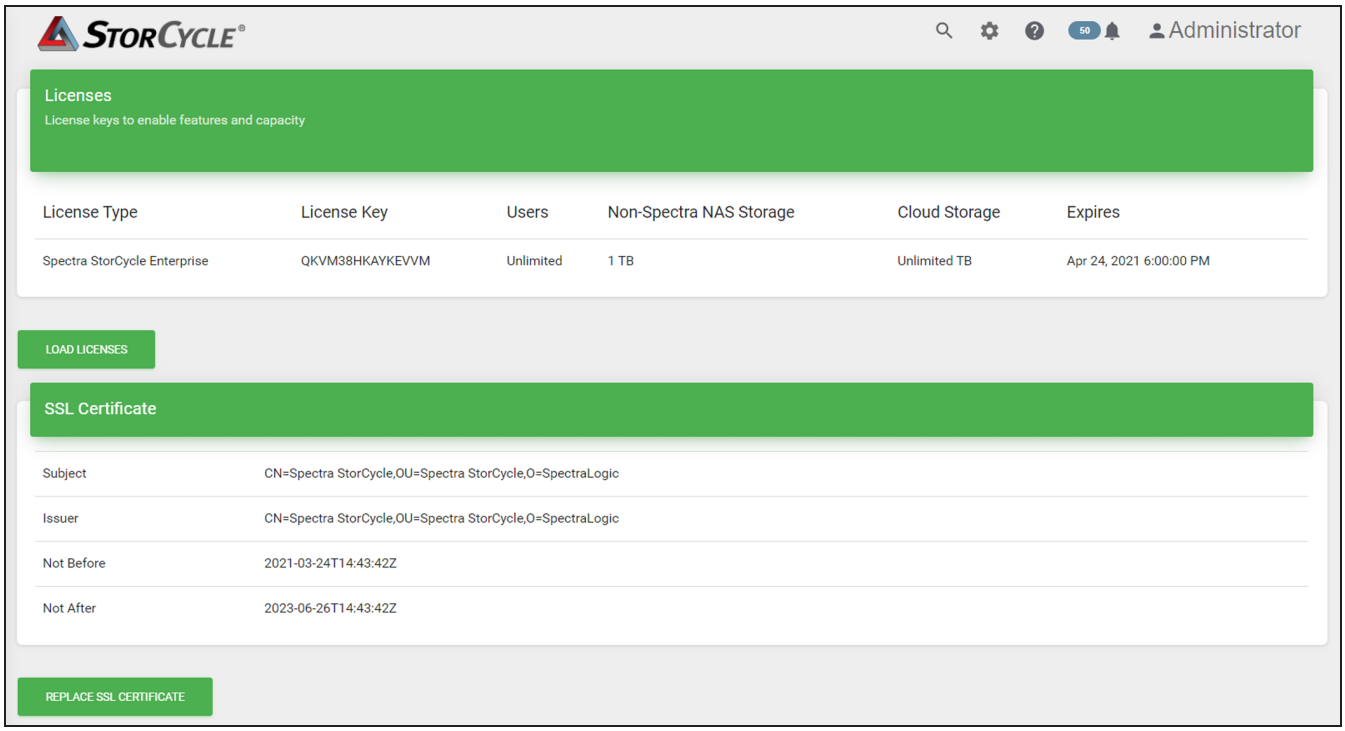


Figure 112 The Licenses & SSL Certificate screen.

Load or Remove License Keys

License keys enable features and capacity within the Spectra StorCycle solution.

Use the following instructions to load or remove license keys.

1. Click **Load Licenses**. The Load Licenses dialog box displays.

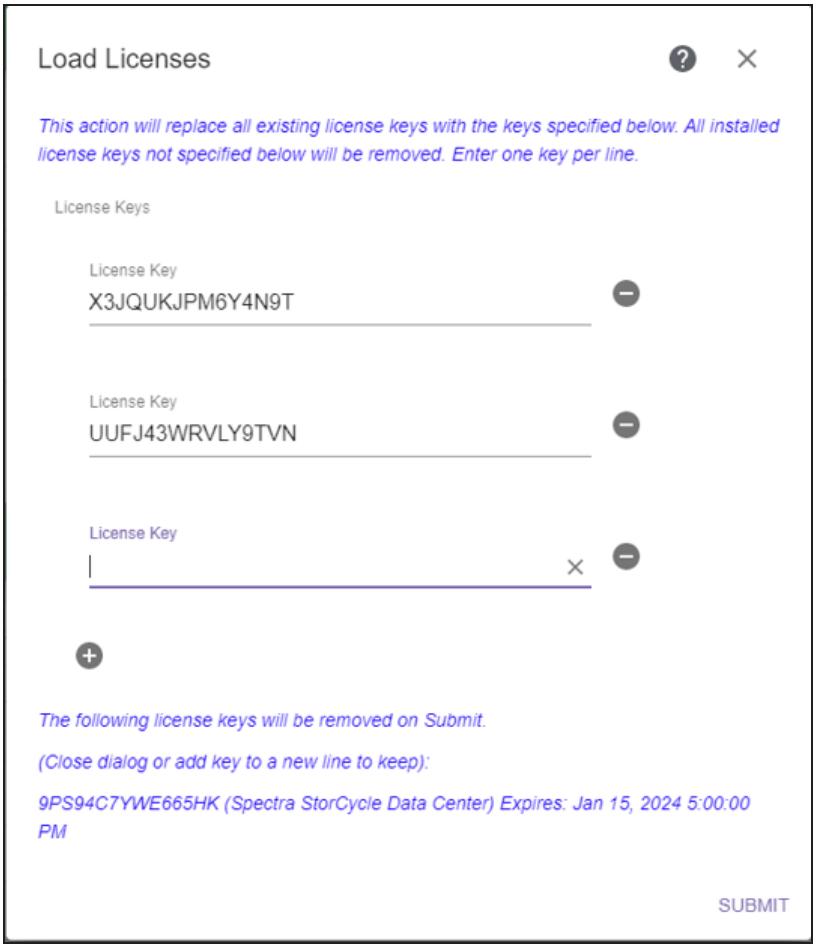


Figure 113 The Load Licenses dialog box.

2. Click the minus (-) sign next to any license that you want to remove.
3. Click the plus (+) sign to add a new line for entering a license. Enter all license keys, exactly as provided, one per line.
4. Click **Submit** to save the license keys. The Licenses & SSL Certificate screen displays with the newly entered keys listed.

Note: When loading or removing license keys, the license wizard displays a brief description of each key being loaded or removed that may include a license key expiration date.

RESET A LOCAL USER PASSWORD

After five unsuccessful login attempts, a local user is locked out of the StorCycle solution.

IMPORTANT Active Directory user login attempts follow Active Directory policies. To protect the Active Directory server, the Spectra StorCycle solution adds a 1 second delay on the next login attempt for every invalid login attempt.

Use the following instructions to reset the password.

Windows Server

1. Sign on to the StorCycle server as a local Administrator.
2. Open a Command Prompt window.
3. Change directory to the StorCycle program directory. The default is: C:\Program Files\Spectra Logic Corporation\Spectra StorCycle.
4. Execute `ssc.exe user reset <username> <password>`, where the *username* is for the user requiring a password reset, and *password* is the new password.

Linux Server

1. Log in to the StorCycle server as a user with sudo privileges.
2. Open a terminal window.
3. Execute `sudo /usr/sbin/ssc user reset <username> <password>` where the *username* is for the user requiring a password reset, and *password* is the new password.

Restore the Database from a Backup

CAUTION To minimize the possibility of losing data migrated / stored since the last database backup was created, contact Spectra Logic Technical Support (see Contacting Spectra Logic on page 9) before using the instructions in this section to restore the database from a backup.

IMPORTANT Database backups are specific to each operating system. Database backups and the Database Archive and Restore actions cannot be used to migrate the database across operating system server platforms. For example, you cannot restore a database to a Windows system if it was originally created by a Linux system, and vice versa.

Use the following instructions to restore a database from a database backup. Database restorations are typically performed when a system is damaged or upgraded.

Windows Server

1. Re-install the StorCycle software. See Download and Install the StorCycle Software on page 57. Make note of the installation directory.
2. Stop the StorCycle service. Navigate to the Services screen. Select the StorCycle Service. Click the **Stop Service** button in the upper left corner of the screen.
3. Find the database backup file. In your destination storage locations, look for backup files which are named ssc-*nodeId-hh-mm-ss*Z.zip. The file with the latest date code is the most recent backup.
4. Unzip the database backup file.
5. Open a Command Prompt window as an administrator and change directory to the StorCycle install directory used in Step 1 on page 225.
6. Execute `ssc.exe database restore <path to unzipped database directory>`.

   Note: Use `database restore --help` to view help for the command.
7. Restart the StorCycle service. Navigate to the Services screen. Select the StorCycle Service. Click the **Start Service** button in the upper left corner of the screen.

Linux Server

1. Ensure the Mongo database repository is updated and compatible. See Create the StorCycle Mongo Database Repository on page 68.
2. Re-install the StorCycle software. See Install the StorCycle Solution on page 70. Make note of the installation directory.

3. Find the database backup file. In your destination storage locations, look for the *ssc-db-backup* directory. The backup files are named ssc-*nodeId-hh-mm-ss*Z.zip. The file with the latest date code is the most recent backup.
4. Unzip the database backup file.

   ```
   unzip -d target_directory -u -q the_database_zip_file
   ```

5. Stop the StorCycle service.

   If you are the root user, execute:

   ```
   systemctl stop ssc
   ```

   If you are a user who has root access, execute:

   ```
   sudo systemctl stop ssc
   ```

   To check that the StorCycle service has stopped, execute:

   ```
   sudo systemctl status ssc
   ```

6. If you are the root user, execute:

   ```
   /usr/sbin/ssc database restore <path to unzipped database directory>/ssc-xxxxxxZ
   ```

   If you are a user who has root access, execute:

   ```
   sudo /usr/sbin/ssc database restore <path to unzipped database directory>/ssc-xxxxxxZ.
   ```

   You will be prompted to enter the root password.

Note: Use `/usr/sbin/ssc database restore --help` to view help for the command.

7. Restart the StorCycle service.

Chapter 11 - Monitor the StorCycle Solution

This section provides instructions for monitoring the Spectra StorCycle solution.

StorCycle Dashboard

View the Dashboard by clicking Dashboard in the taskbar. For information on using the embedded BlackPearl dashboard, see Embedded BlackPearl Dashboard on page 250.

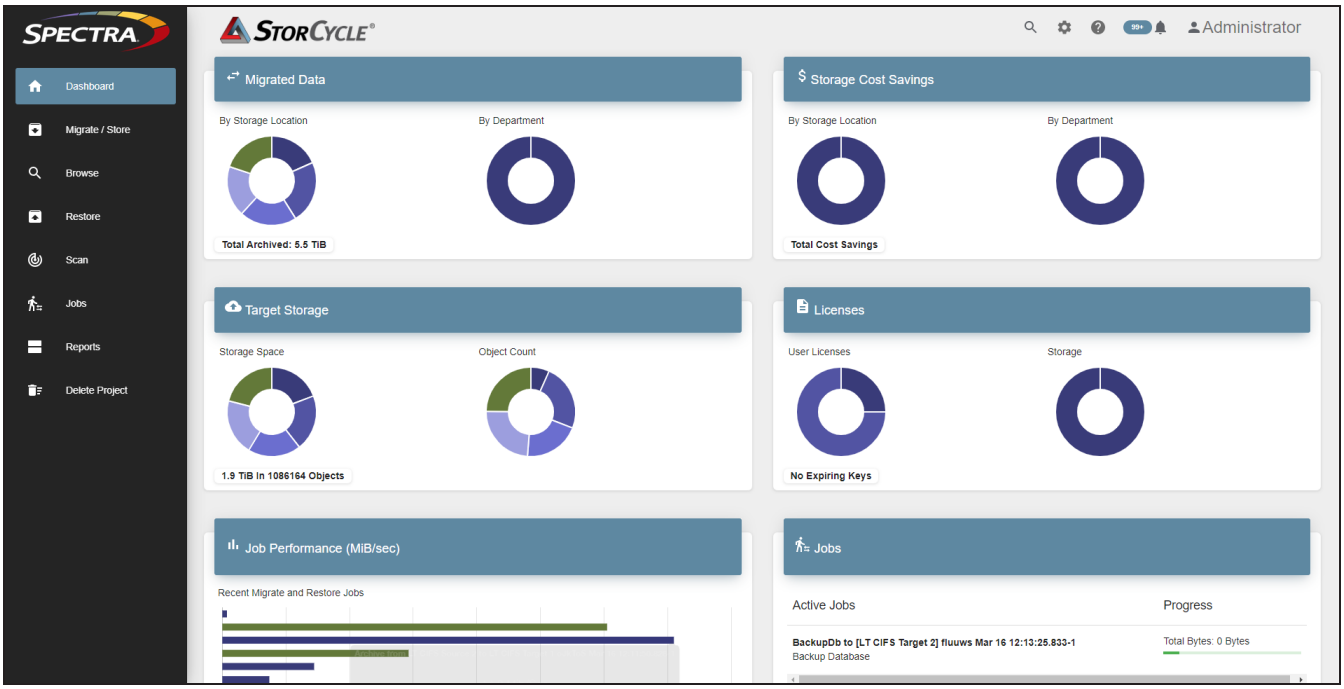


Figure 114 The Dashboard screen.

The dashboard provides a quick graphical display of available resources and cost saving gained by using the StorCycle solution. More detail can be seen in StorCycle reports (see Reports on page 237).

Migrated Data — The Migrated Data pane displays the amount of data migrated by source storage location, and if departments are configured, by department. Hovering your mouse over a colored section of a graph displays the storage location or department represented by the color and the associated amount of data. Clicking a pane displays a table representation of the information in the two graphs.

Storage Cost Savings — The Storage Cost Savings pane displays the money saved by transferring data from high cost primary storage to lower cost secondary storage. If Cost/TiB or Department is not entered for storage locations (see Storage on page 81), this section displays zero cost savings. Hovering your mouse over a colored section of a graph displays the storage location or department represented by the color and the associated cost savings. Clicking the pane displays a table representation of the information in the two graphs.

Target Storage — The Target Storage pane displays the used space and object count on target Storage Locations. Hovering your mouse over a colored section of a graph displays the storage location or object count represented by the color and the associated amount of data or count. Clicking the pane displays a table representation of the information in the two graphs.

Licenses — The License pane displays the available and used licensed users and non-Spectra storage, and the license key expiration date. Hovering your mouse over a colored section of a graph displays the number of users licensed and used or the amount of data licensed or used. Clicking the pane displays a table representation of the information in the two graphs. The background color for the Next Key Expiration information indicates how soon the key expires.

- **White** — More than 30 days.
- **Yellow** — Less than 30 days.
- **Red** — Expired.

Job Performance — The Job Performance pane displays the MiB/s performance for recent jobs. Hovering your mouse over a bar in the graph displays the job associated with the performance number. Clicking the pane displays a table representation of the information in the graph.

It also displays the date and time for the last successful Database Backup. The background color for the Database Backup status indicates the age of the last successful backup.

- **White** — Less than one day old.
- **Yellow** — One to seven days old.
- **Red** — Greater than seven days old.

Clicking the database backup summary information takes you to the Database Backup dashboard (see Database Backup on page 128).

Jobs - The Jobs pane displays currently active jobs with their progress, and any queued jobs. Queued jobs can be promoted to the next job to run by clicking the **Run** icon next to the job name.

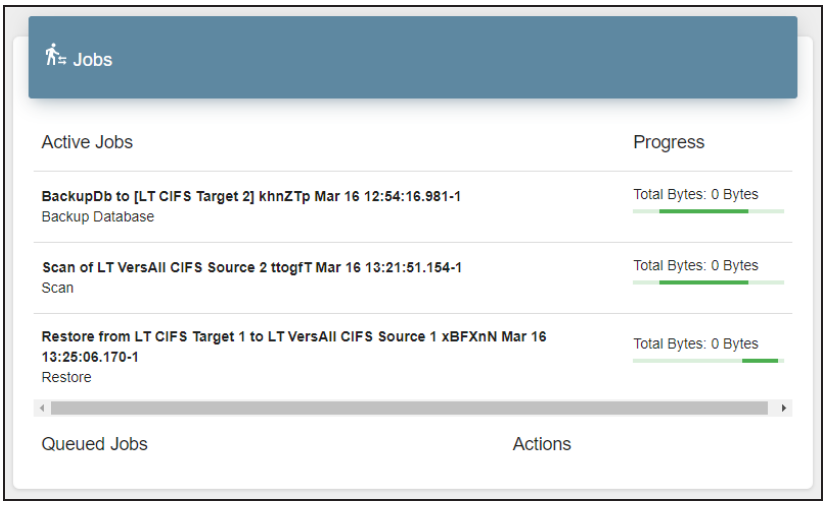


Figure 115 The Jobs pane.

Completed Scans — The bottom of the dashboard displays graphs showing the breakdown of the age and size of the files in each storage location based on the cumulative scan per location. See Scanning Overview on page 150 for more information on how scan graphs are created and updated.

JOBS

Select **Jobs** to display the Recent Jobs screen.

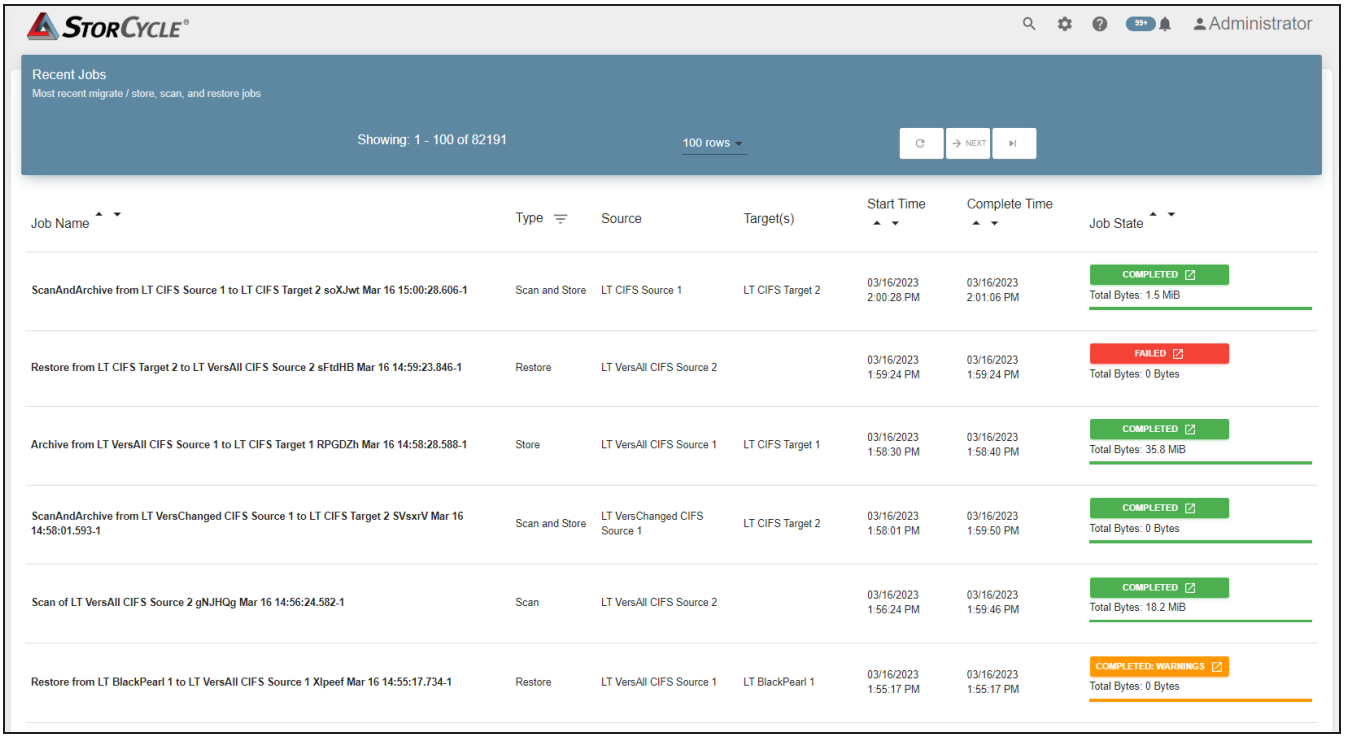


Figure 116 The Recent Jobs screen.

Notes:

- While the job is active, hovering over the total bytes for the job in the Job State column displays the job performance.

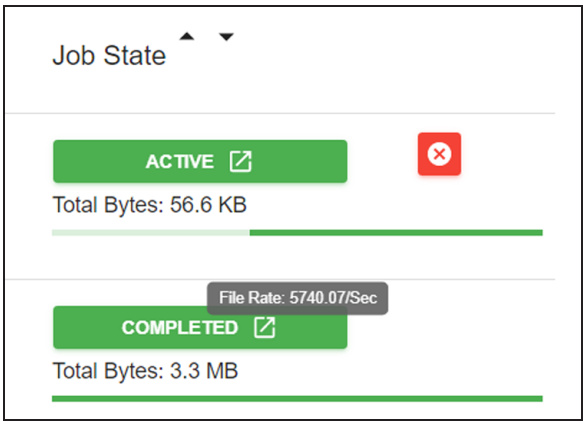


Figure 117 Job performance for a scan job.

- The Scan, Migrate / Store, and Restore Dashboards also display recent jobs of the corresponding type.

The Recent Jobs screen displays the following information:

Heading	Description
Job Name	The name of the job. The name uses the Project name defined when configuring the project and a number indicating how many times the project was previously run.
Type	The type of job. Values include Backup Database, Restore, Retention Delete, Scan, Scan and Store, Store, and Version Delete.
Source	The storage location used as the source for the job. **Note:** This will be empty for a database backup.
Target(s)	The storage location(s) used as the target(s) for the job. **Note:** This will be empty for Scan, Restore, Retention Delete, or Version Delete jobs or migrate / store jobs that have been deleted.
Start Time	The date and time the job started.
Complete Time	The date and time the job completed.
Job State	The status of the job. Values include: Active, Canceled, Canceling, Completed, Completed: Errors, Completed: Warnings, Deleted, and Failed.

Job Details

Click the ***Job Name*** or the ***Job State*** to display the Job Details dialog box.

Note: Job Details can also be seen by clicking the ***Job Name*** or the ***Job State*** in the Jobs section on the Scan, Migrate / Store, or Restore screen.

Select:

- The **Job Details - Job Tab** tab
- The **Job Details - Project Tab on page 233** tab
- The **Job Details - Histogram Data Tab on page 234** tab.

Note: Delete jobs created by retention policies do not include a **Project** tab.

Job Details - Job Tab

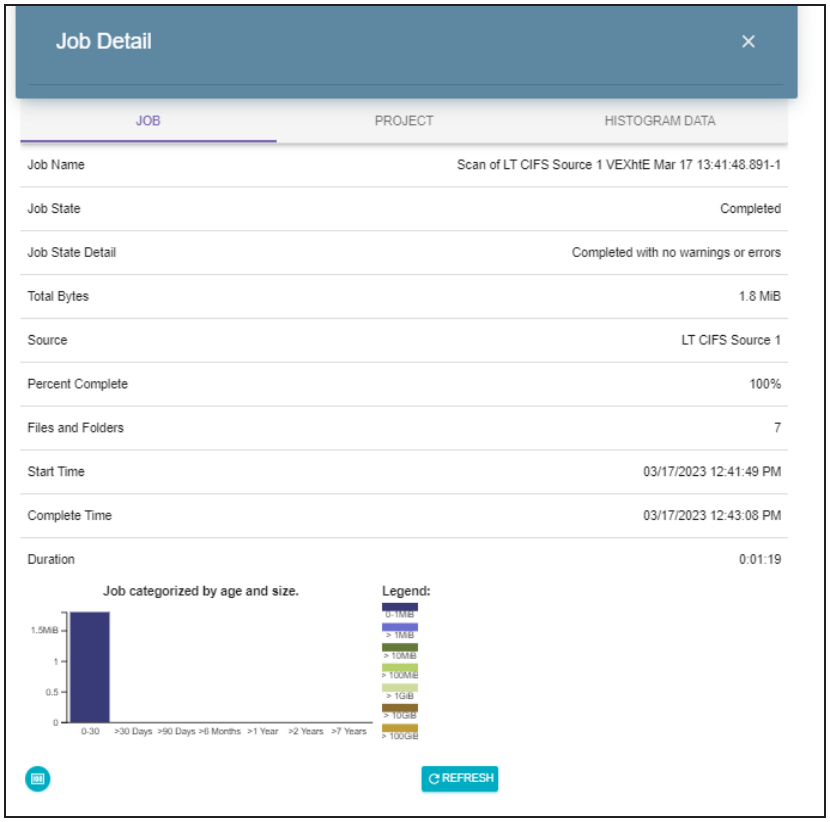


Figure 118 The Job Detail - Job tab for a scan and store job.

The information presented in the Job Detail dialog box varies depending on the job type, and can include the following:

Heading	Description
Job Name	The name of the job.
Job State	The status of the job. Values include: Active, Canceled, Canceling, Completed, Completed: Errors, Completed: Warnings, and Failed.
Job State Detail	Whether a job completed with warnings, errors, or neither; failed with warnings, errors, or neither, or was canceled with warnings, errors, or neither.
Total Bytes	The number of bytes of data that were processed and the percent complete.
Source	The storage location used as the source for the job.
Target(s)	The storage location(s) used as the target(s) for the job.

Heading	Description
Percent Complete	The percent of the overall job which is complete.
Files and Folders	The number of files and folders that were processed.
Start Time	The date and time the job started.
Complete Time	The date and time the job completed.
Duration	How long the job took to complete in the format *hh*:*mm*:*ss*, where *hh* is the number of hours, *mm* is the number of minutes, and *ss* is the number of seconds.
Catalog	The name of the catalog containing the information about the migrated / stored data.
Warnings and Errors if applicable	Warnings and errors generated by the job display at the bottom of the Job Details.

Job Details - Project Tab

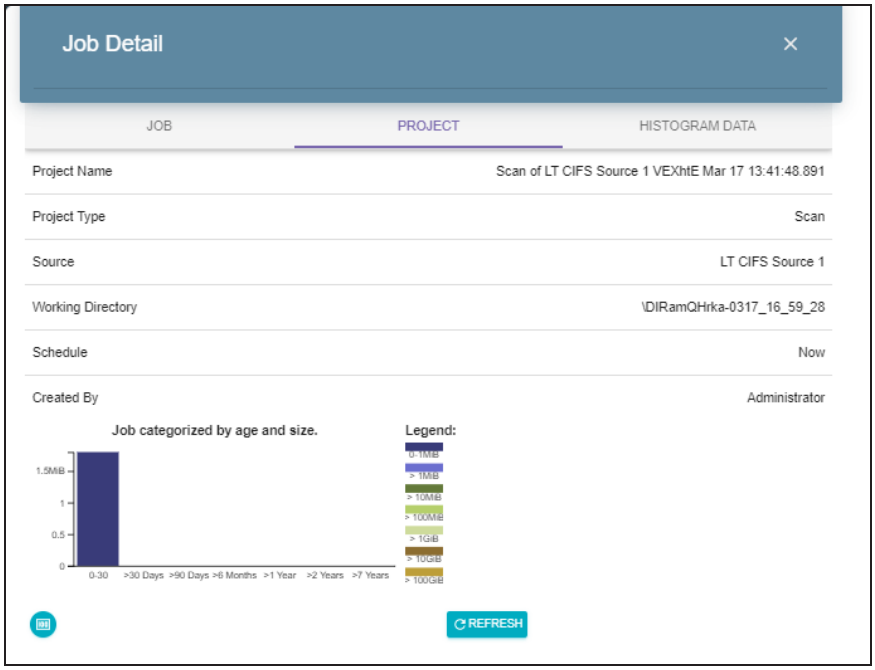


Figure 119 The Job Detail - Project tab for a scan and store job.

The Job Detail - Project tab displays the information entered when creating the project. The information varies depending on the project type. See Create a Scan Project on page 157, Create a Migrate / Store Project on page 166, or Create a Restore Project on page 191 for a description of the settings.

Job Details - Histogram Data Tab

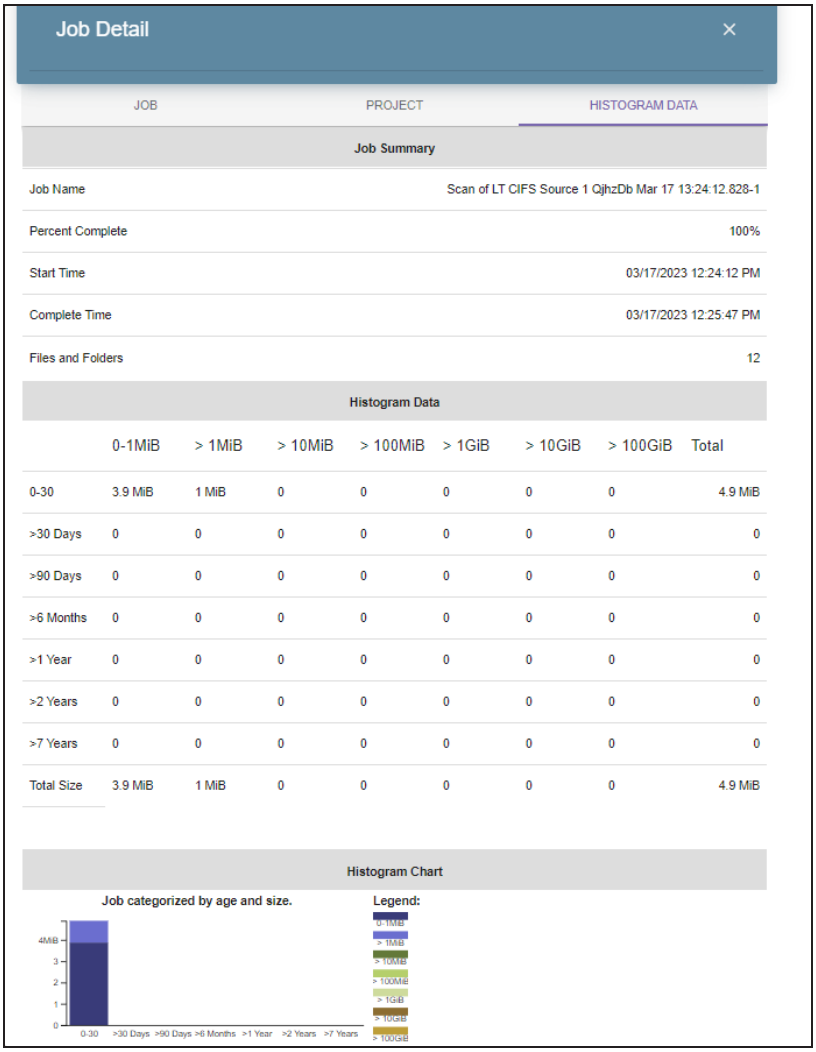


Figure 120 The Job Detail - Histogram Data tab for a scan and store job.

The Job Detail - Histogram Data tab displays a tabular representation of the histogram.

Savings Calculator

Click **Savings Calculator** at the bottom of a Scan Job Detail dialog box to display the Savings Calculator.

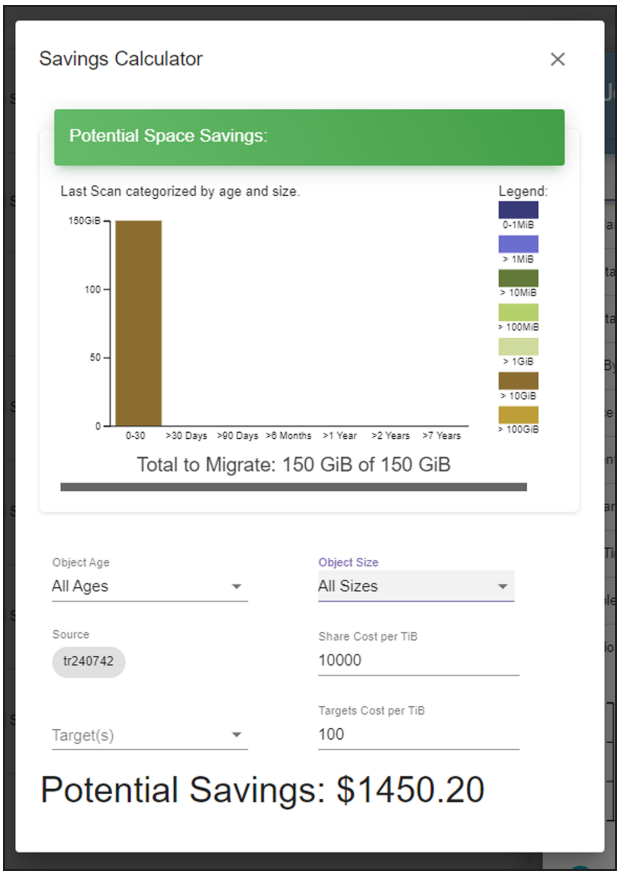


Figure 121 The Savings Calculator.

1. Using the **Object Age** drop-down, select the age of files to include.

Notes:
- **Object Age** is determined using the configured **Method to determine file age**. See Configure Global Settings on page 135 for more information.
- Only those objects meeting the **Object Age** and the **Object Size** requirements are included.

2. Using the **Object Size** drop-down, select size of files to include.

Note: Only those objects meeting the **Object Age** and the **Object Size** requirements are included.

3. The **Source** and **Share Cost per TiB** are entered automatically with the source of the job and the Cost/TiB entered when creating the source storage location. The **Share Cost per TiB** can be altered in the Savings Calculator. Making changes to the **Share Cost per TiB** in the Savings Calculator does not change the value set for the storage location.

4. If desired, select one or more **Target(s)**. The **Targets Cost per TiB** updates to display the total of the Cost/TiB entered for all selected **Target(s)**. The **Targets Cost per TiB** can be altered in the Savings Calculator. Making changes to the **Targets Cost per TiB** in the Savings Calculator does not change the value(s) set for the storage location(s).
5. The **Potential Savings** value indicates how much you can save by moving the selected files from primary storage to secondary storage.

REPORTS

The StorCycle solution includes an extensive Reports section to allow users to get the most from their investment. All reports are visible in the web interface and are exportable to Comma Separated Value (CSV) and Javascript Object Notation (JSON) format.

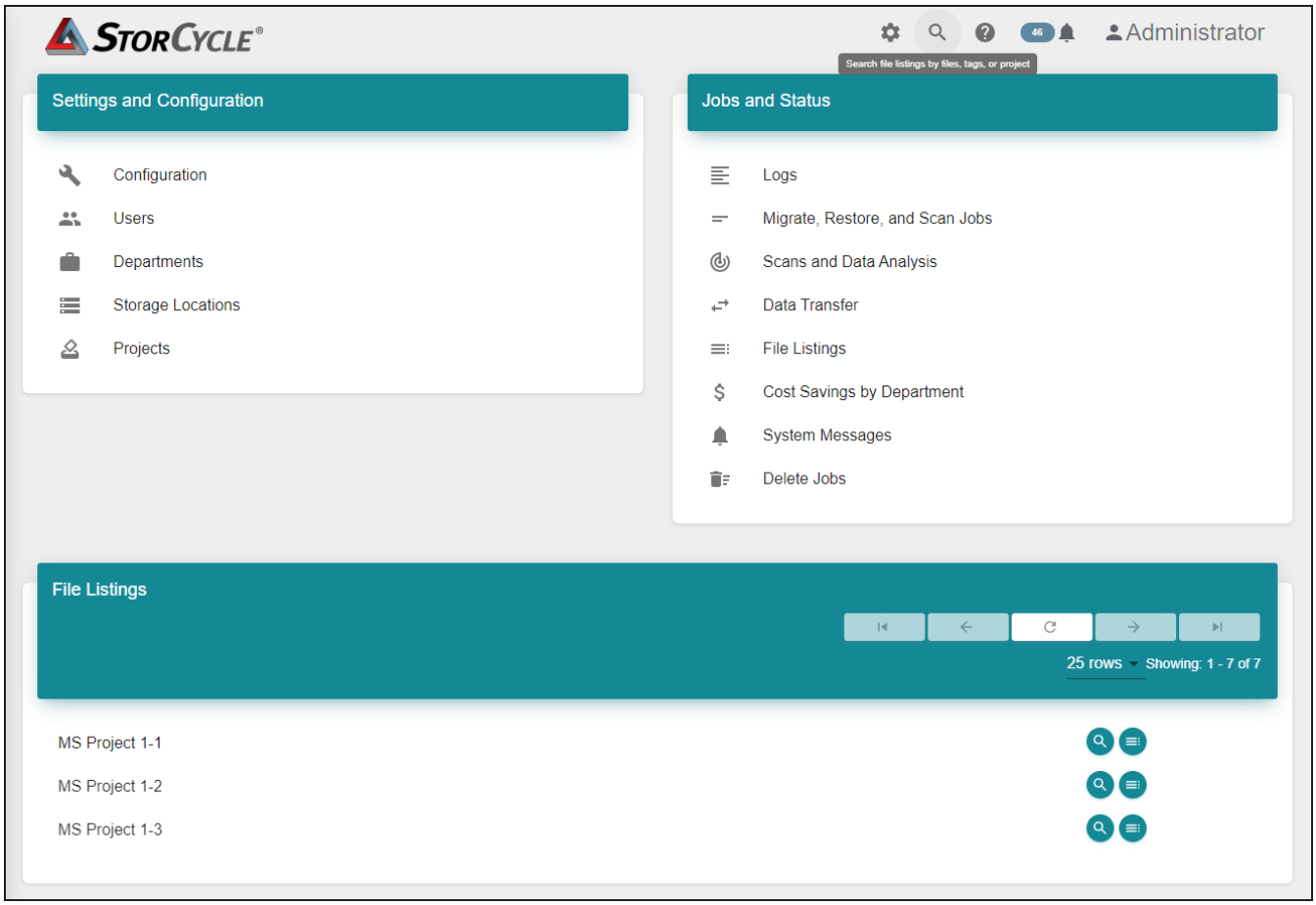


Figure 122 The Reports screen.

Reports are provided in three major categories:

Settings and Configuration — Configuration information, such as software version; Users; Departments; Storage Location settings; Projects.

Jobs and Status — Logs; Migrate / Store, Restore, and Scan Jobs; Scans and Data Analysis; Data Transfer; Catalogs (list); Cost Savings by Department; System Messages; Delete Jobs.

File Listings — List of migration / store projects. Click **Details** to see the name, description, created time, updated time, type, created by, and project name information for the project. Click **List** to see a list of objects included in the project and the original path, whether it was a directory, the size, and the checksum for the object.

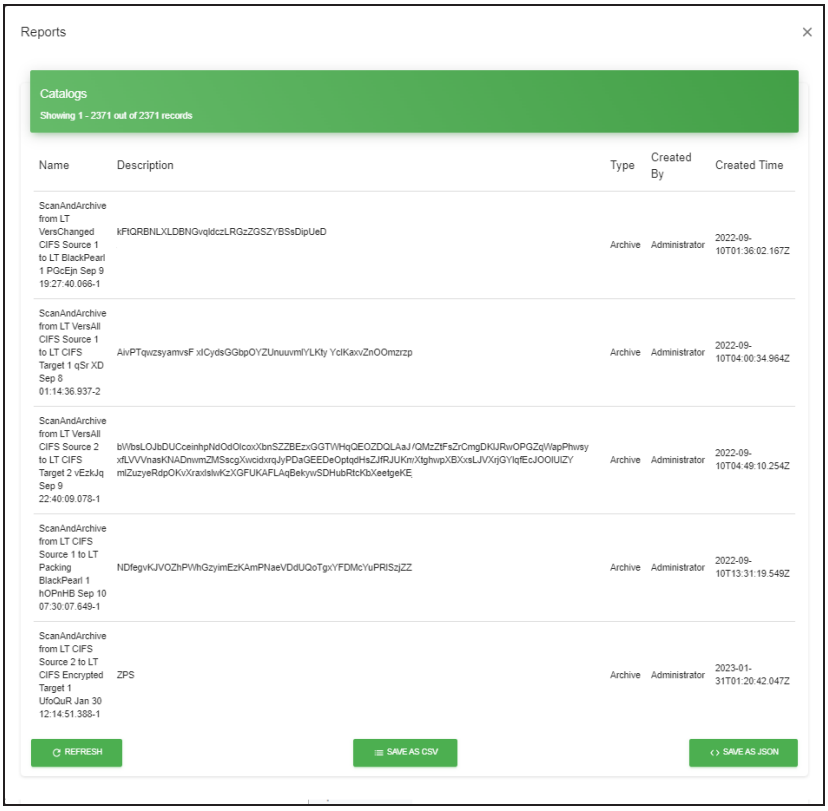


Figure 123 The Catalog File Listing screen.

Click **Save as CSV** or **Save as JSON** at the bottom of the list to save the list.

System Messages

System messages provide important information about the Spectra StorCycle solution operation. Reviewing the messages is the first step in troubleshooting.

Note: To have messages sent by email to users, see Configure Users on page 142.

To view messages, click **Message** in the toolbar.

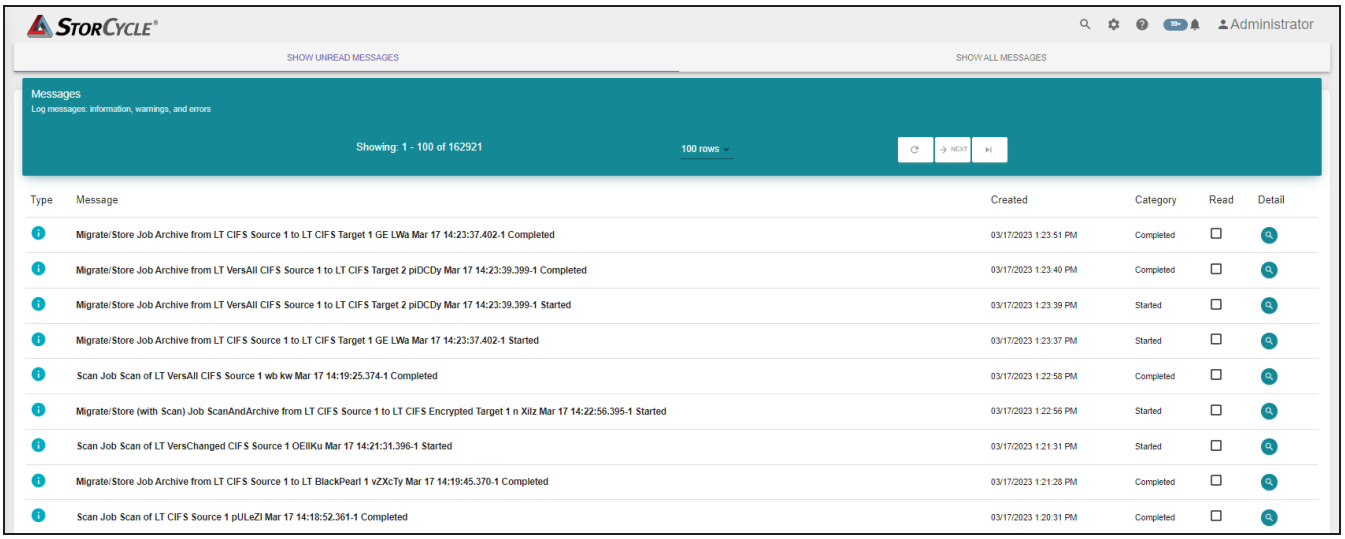


Figure 124 The Messages screen.

Select the **Show Unread Messages** or **Show All Messages** tab.

The messages are categorized as:

- **Info** - An expected event occurred such as a job starting or completing successfully.
- **Warning** - A job completed with warnings or errors, for example, a file to be migrated / stored was already migrated / stored, therefore, it was skipped. Determine the cause of the problem and remedy it if necessary.
- **Error** - A job failed with warnings or errors, for example, the StorCycle solution cannot communicate with a storage location. Determine the cause of the error and remedy it as soon as possible.

Mark Messages as Read

To mark an individual message as read, select the **Read** check box.

To mark all messages as read, click **Mark All As Read** at the bottom of the Messages screen.

View Message Details

To see more detail about a message, click **Details** to the right of the message. The Message Details screen displays.

Note: Some sections of the Message Details use local time and some use UTC, each marked accordingly.

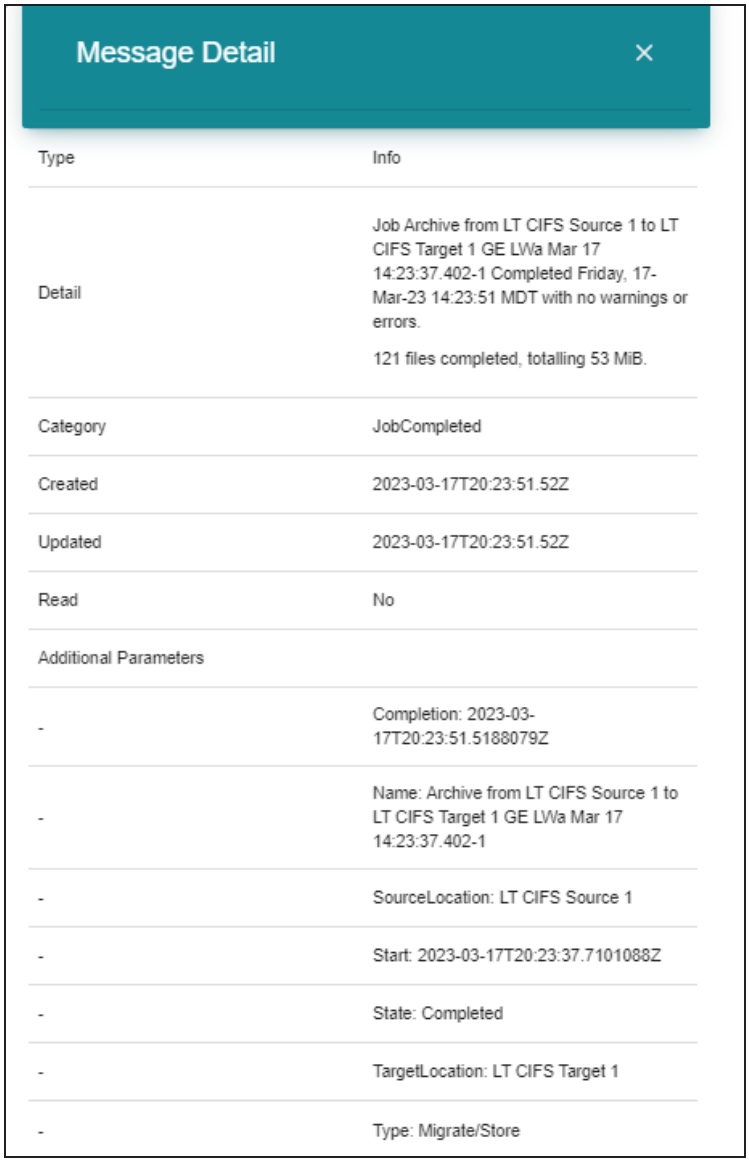


Figure 125 The Message Details dialog box.

Logs

The Spectra StorCycle solution automatically creates error logs and writes event information into log files for troubleshooting purposes. When one of the log files reaches 10 MiB in size, the log file text is written to a timestamped file and the existing log file is cleared. Up to ten, 10 MiB files of each type are stored on the server. A log set, which gathers the current log of each type, can be generated manually.

Note: The current log file is not cleared when a log set is created. If one log set is created and then a second log set is created before the log file reaches 10 MiB in size and is cleared, the two log sets will have overlapping information.

Click **Settings** in the toolbar and then select **Logs**. The Logs screen displays showing the currently saved log sets.

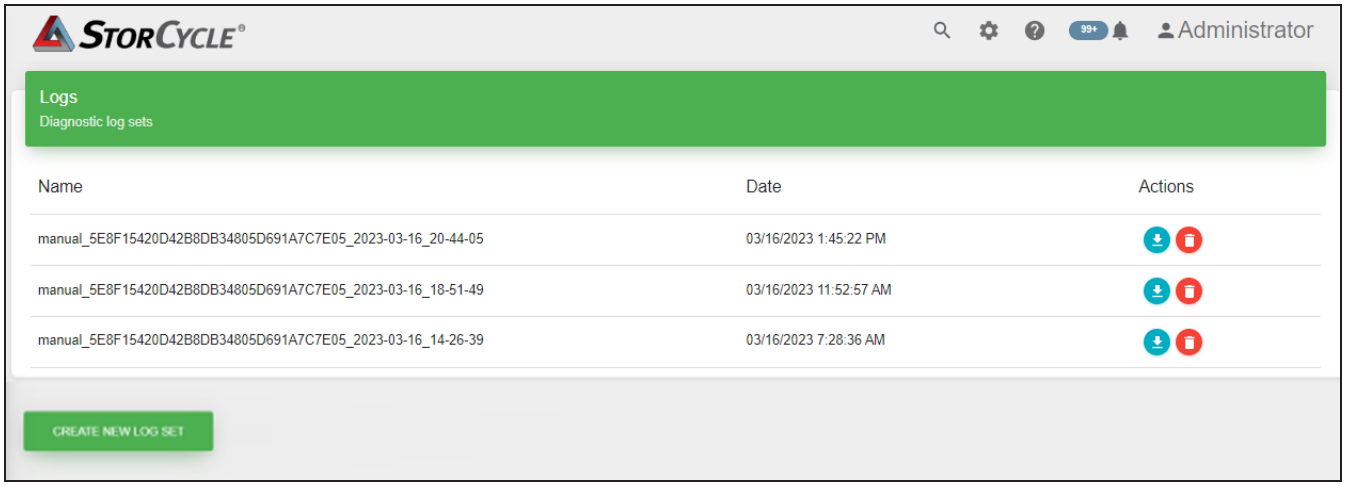


Figure 126 The Logs screen.

Create a Log Set

1. Click **Create New Log Set**. The Create New Log Set dialog box displays.

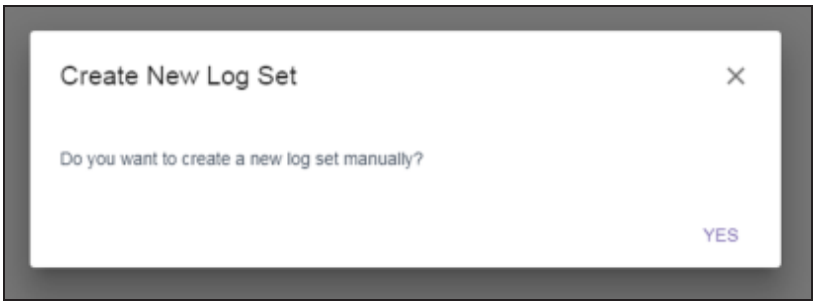


Figure 127 The Create New Log Set dialog box.

2. Click **Yes**. A new log set is collected immediately.

Download a Log Set

To download a log set, click **Download** next to the log set that you want to download. The log set begins downloading to your host computer.

Delete a Log Set

To delete a log set, click **Delete** next to the log set that you want to delete. Click **Delete** to confirm the deletion.

Note: Deleting a log set does not delete the log files, just the gathered set of log files.

Chapter 11 - Upgrade or Remove The StorCycle Solution

This section provides instructions for upgrading the Spectra StorCycle solution software to a new version, and instructions on removing the software.

UPGRADE THE STORCYCLE SOLUTION

Use the following instructions to upgrade the StorCycle solution to a new version.

IMPORTANT Spectra Logic strongly recommends that you create a database backup before upgrading the software. See Database Backup on page 128.

Notes:
- Program data is retained with an upgrade.
- Downgrading is not supported.

Windows Server

Use the following instructions to download and install the new version of software on a Windows server.

1. Sign in to the server where you want the program to run as a user that is a member of the "Administrators" Local Group.
2. Download the Spectra StorCycle solution installer.
3. Run the installer, `ssc.`*`revision`*`.msi`, where *`revision`* is the revision number for the software.
4. Follow the on-screen instructions to install the software. Leave the **Account name** and **Password** fields empty to run the StorCycle service using the previously configured account.

Linux Server

When upgrading the StorCycle solution, in some cases, you cannot upgrade directly from your current version to the newest version. The StorCycle solution requires that you upgrade to all intermediate StorCycle versions with unique MongoDB versions between your current version and your target StorCycle version. You cannot skip a StorCycle version if the MongoDB version changes between your current and target StorCycle version.

For example, as shown in the table below, you can upgrade from StorCycle 3.6.2 to 3.7.1 directly, skipping version 3.7.0, because the version of MongoDB required for those versions of StorCycle does not change.

However you cannot upgrade directly, from version 4.0.0 to version 4.3.0 as the MongoDB version is not the same between both versions. You would first need to upgrade from StorCycle version 4.0.0 to 4.1.0, then 4.1.0 to 4.2.0, and finally from 4.2.0 to 4.3.0. During each of those upgrades, you also must upgrade the MongoDB repo. You cannot skip upgrading the MongoDB when installing a newer version of the StorCycle solution. Both must be upgraded in sequence to allow for proper database conversion.

Use the following instructions to download and install the new version of software on a Linux server.

1. Update your MongoDB repository. Use the table below to determine the supported version of MongoDB.

StorCycle Version Number	MongoDB Version Number
3.6.2	MongoDB 4.0
3.7.0	MongoDB 4.0
3.7.1	MongoDB 4.0
4.0.0	MongoDB 4.2
4.1.0	MongoDB 4.4
4.2.0	MongoDB 5.0
4.3.0	MongoDB 6.0

2. Open the terminal and sign in as a superuser.

Note: The following commands reflect upgrading to StorCycle version 4.3.0. If you are installing a different version of the software, you will need to adjust the values in red below to the appropriate version listed in the table above.

3. Create a file named:

```
/etc/yum.repos.d/mongodb-org-6.0.repo
```

4. Open the file and enter the following:

```
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/releaseversion/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-6.0.asc
```

5. Obtain the link for the new version from a Spectra representative. Copy the .rpm file to the server where the StorCycle solution will be installed.

6. Navigate to the directory where the .rpm file is located or give the full path to the file. The .rpm must run as root.

7. To install the StorCycle .rpm, use the following command:

```
sudo yum install -y ssc-production-4.3.0.XXX.XXXXXXXX.rpm
```

8. If desired, change the user from root using the following commands:

```
sudo chown -R user:group /var/lib/ssc
sudo vi /usr/lib/systemd/system/ssc.service
# User=root - change root to the new user name
```

REMOVE THE STORCYCLE SOLUTION

When removing the StorCycle solution, no data is removed from storage targets, but records of where data is persisted, and object metadata tags are lost.

Windows Server

Uninstall the StorCycle Software

Use the following instructions to remove the StorCycle solution from a Windows server.

Note: Product configuration, metadata information, license keys, logs, and the product database are not removed when uninstalling the software.

1. Sign into Windows with a user that is a member of the "Administrators" Local Group.
2. Run the installer, `ssc.`*`revision`*`.msi`, where *`revision`* is the revision number for the software. Follow the on-screen instructions to install the software.
3. On the Welcome screen, click **Next**. The Change, repair, or remove installation screen displays.

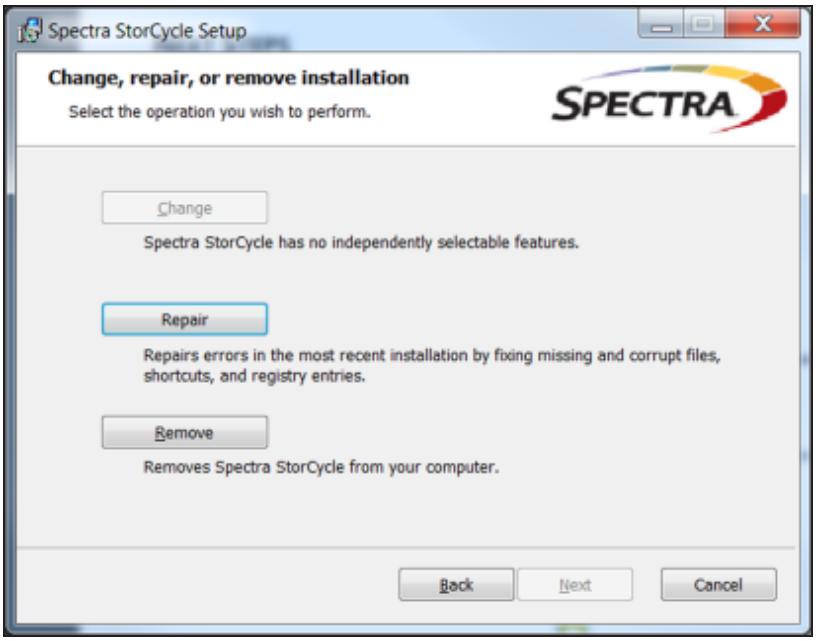


Figure 128 The Change, repair, or remove installation screen.

4. Click **Remove**. A confirmation screen displays.
5. Click **Remove** to confirm the removal.

6. Optionally, if you want to delete the product configuration, metadata information, license keys, logs, and the product database associated with the StorCycle solution, delete the directory C:\ProgramData\Spectra Logic Corporation\Spectra StorCycle. Once deleted, the information **cannot** be recovered.

IMPORTANT If you plan to reinstall the StorCycle solution, Spectra Logic recommends against deleting this data.

Uninstall the MongoDB Service

Optionally, use the following commands to remove the MongoDB service.

1. Use the Services console to stop the service.
   a. Sign in to Windows with a user that is a member of the "Administrators" Local Group.
   b. Use the keyboard shortcut Windows logo key+R to open the Run window.
   c. In the **Open:** field enter `services.msc` and click **OK**. The Services screen displays.
   d. Right-click the MongoDB service and select **Stop**.
2. Open a Windows command prompt as an Administrator, and run the following command:

   ```
   sc.exe delete MongoDB
   ```

Linux Server

Uninstall the StorCycle Software

Use the following instructions to remove the StorCycle solution from a Linux server.

Note: Product configuration, metadata information, license keys, logs, and the product database are not removed when uninstalling the software.

If you are the root user, execute `yum erase ssc`

If you are a user who has root access, execute `sudo yum erase ssc`. You will be prompted to enter the root password.

Uninstall the MongoDB Database

Optionally, use the following commands to remove the MongoDB database.

CAUTION Product configuration, metadata information, license keys, logs, and the product database **are** removed with the MongoDB database.

1. Stop the mongod process by issuing the following command:

   ```
   sudo service mongod stop
   ```

2. Remove any MongoDB packages that you had previously installed.

   ```
   sudo yum erase $(rpm -qa | grep mongodb-org)
   ```

3. Remove MongoDB databases and log files.

   ```
   sudo rm -r /var/log/mongodb
   sudo rm -r /var/lib/mongo
   ```

Remove Configuration and History Information

Optionally, use the following command to remove StorCycle configuration and history information.

```
sudo rm /var/lib/ssc
```

Chapter 12 - Embedded BlackPearl Dashboard

This chapter describes the embedded dashboard of the BlackPearl management interface. The embedded dashboard is used by the StorCycle Solution to display an overview of the BlackPearl system, display jobs, tape management, and other common functions. However, the embedded dashboard may be used separately for certain tasks in place of the BlackPearl management console.

ACCESSING THE EMBEDDED BLACKPEARL DASHBOARD

To access a previously configured BlackPearl storage location and view the embedded dashboard, select the **Settings** menu and select **BlackPearl**. The Storage screen displays with only BlackPearl storage locations displayed.

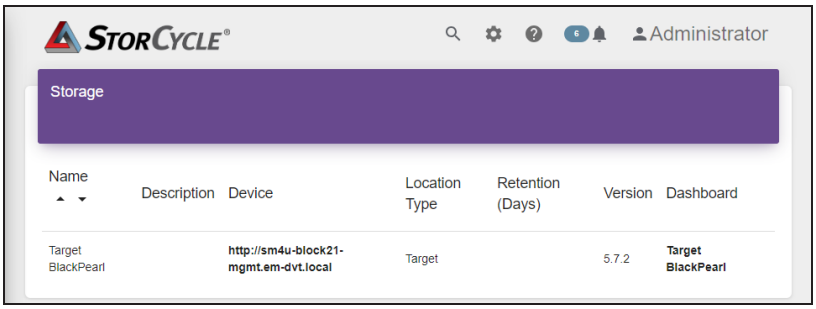


Figure 129 The Storage screen.

The Storage screen lists configured BlackPearl storage locations along with their description, device link, location type, retention policy, BlackPearl OS version, and dashboard.

To access the embedded dashboard, click the link in the **Dashboard** column.

Note: In order to access the embedded BlackPearl dashboard, the BlackPearl system must be running BlackPearlOS 5.7.0, or later.

USING THE EMBEDDED DASHBOARD

The embedded dashboard allows you to quickly view the status of critical aspects of the BlackPearl system and easily perform commonly used functions of the system.

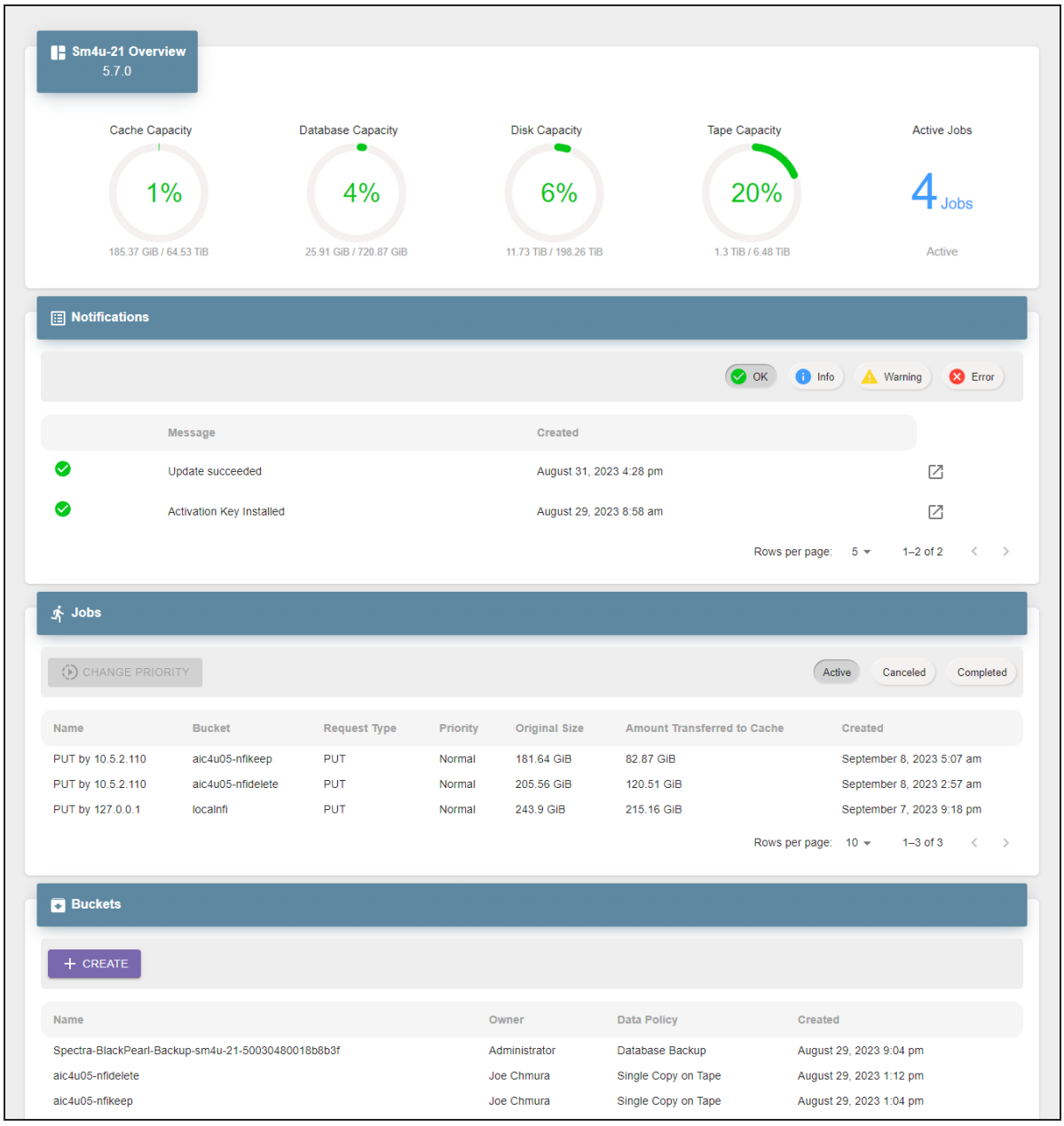


Figure 130 The Embedded Dashboard.

VIEW THE STATUS OF THE BLACKPEARL SYSTEM

Use the sections below to view the status of multiple aspects of the BlackPearl system.

View System Overview

The Overview pane provides a quick look at the most critical aspects of the BlackPearl system.

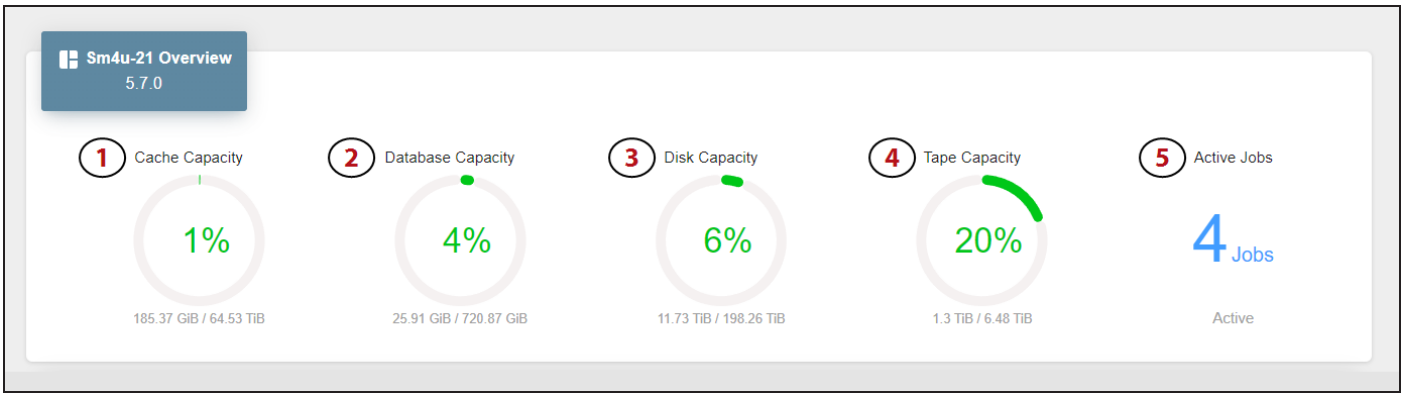


Figure 131 The Overview pane.

1. The BlackPearl cache capacity and percentage of used cache space.
2. The capacity of the BlackPearl database and percentage of used space.
3. The capacity of all disk-based storage connected to the BlackPearl system and percentage of used space.
4. The capacity of all tape-based storage in the tape library connected to the BlackPearl system and percentage of used space.
5. The number of active jobs running on the BlackPearl system.

Mouse-over the green section of any percentage graph to display the amount of used space, and over the gray section to display the amount of remaining space.

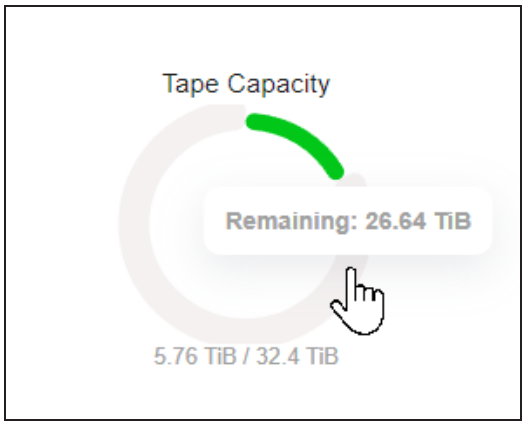


Figure 132 Mouse-over a graph to view specific details.

View Notifications

Notifications provide information about errors that occur on the system, caution messages that alert you to issues that may impact your workflow, and informational messages. Additionally, notifications may provide troubleshooting advice to help you resolve issues that may occur.

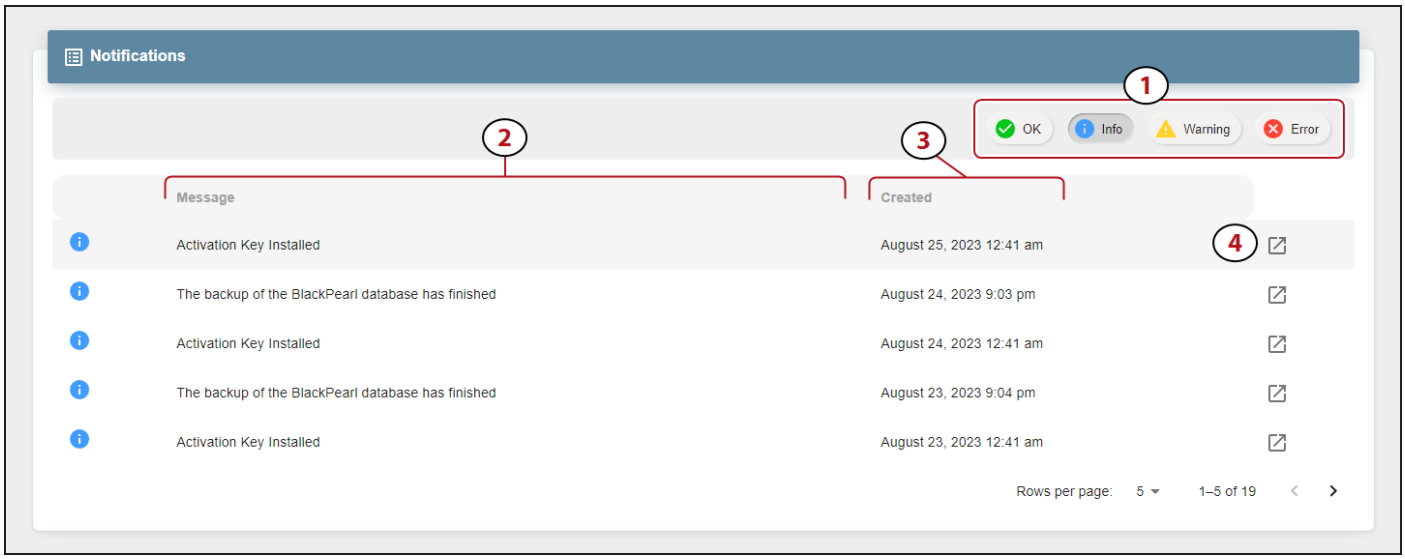


Figure 133 The Notifications pane.

1. Use the **Notification Type** buttons to switch between OK, Info, Warning, and Error messages.
2. Contains a brief description of the notification.
3. Displays the timestamp the notification was generated.
4. Click the **Details Button** to view additional message **Details** and **Troubleshooting Advice**.

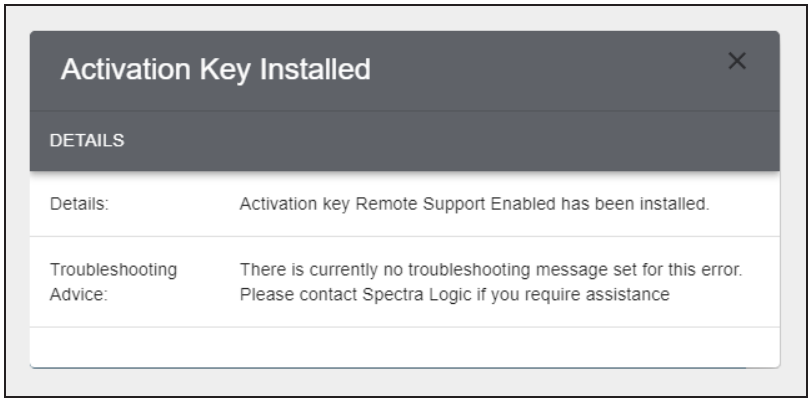


Figure 134 The Notification details dialog box.

View Jobs

The Jobs pane provides information on each Active, Canceled, or Completed job processed by the BlackPearl system.

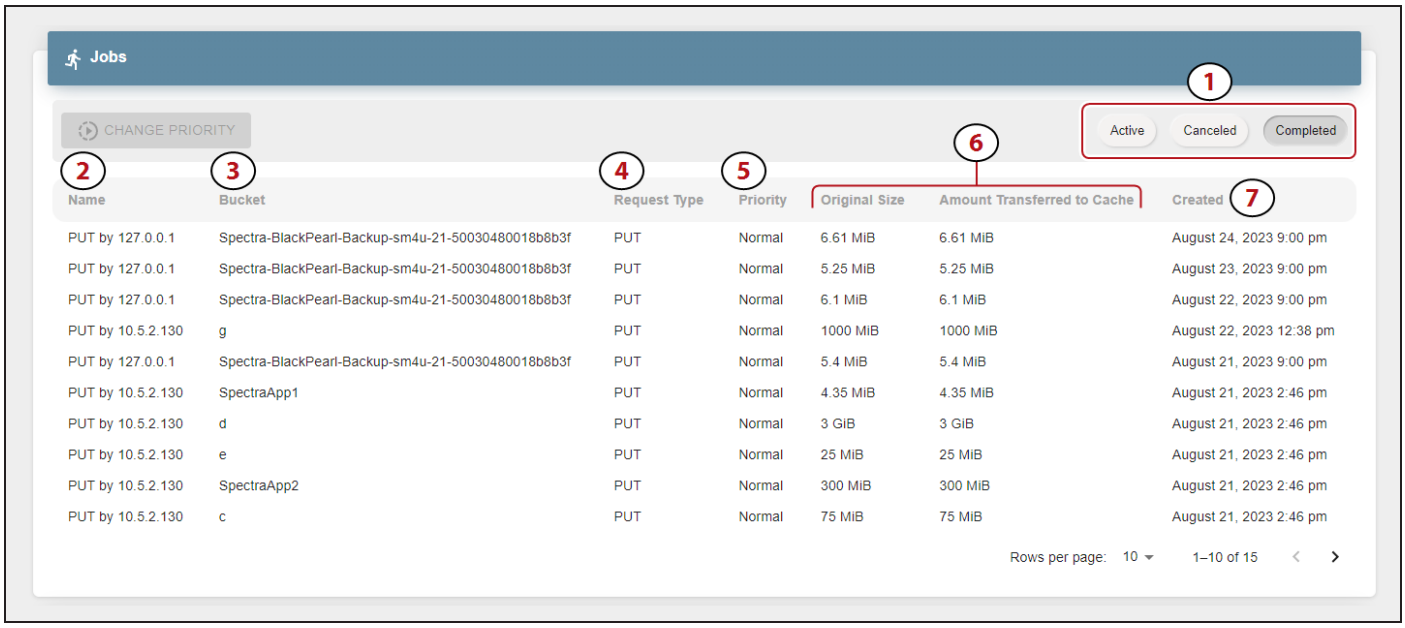


Figure 135 The Jobs pane.

1. Use the **Job Type** buttons to switch between Active, Canceled, and Completed jobs.
2. The name of the job includes the job type and the IP address of the job initiator.
3. The bucket used in the PUT or GET operation.
4. The type of job request.
5. The assigned priority of the job.
6. The original size and amount of data transferred to the BlackPearl cache.
7. Displays the timestamp of when the job was initiated.

Use the **Change Priority** button to change the priority of an active job. See Change Job Priority on page 265 for more information.

View Buckets

The Buckets pane provides information about all buckets configured on the BlackPearl system.

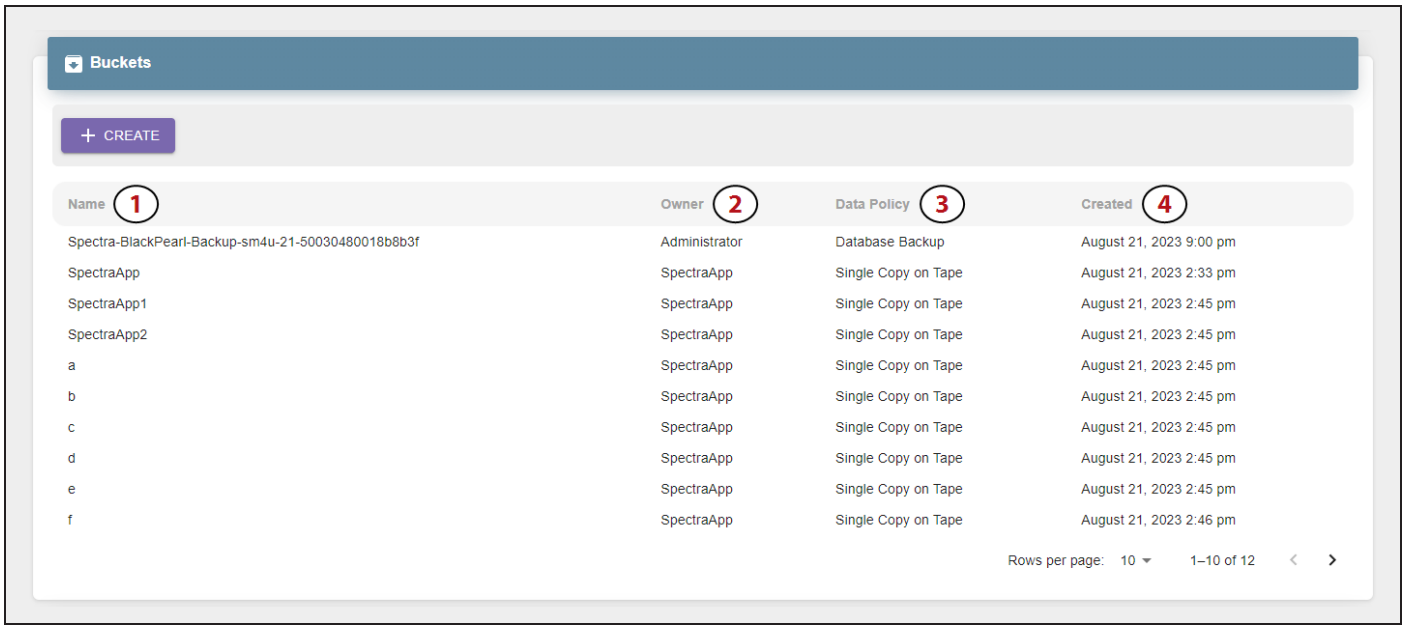


Figure 136 The Buckets pane.

1. Displays the name of the bucket
2. The bucket owner configured on the BlackPearl system.
3. The data policy used by the bucket.
4. Displays the timestamp of when the bucket was created.

The **Create** button to create a new bucket. See Create a Bucket on page 265 for instructions.

View Pools

The Pools pane displays information about all disk storage pools configured on the BlackPearl system including dedicated BlackPearl cache and database pools.

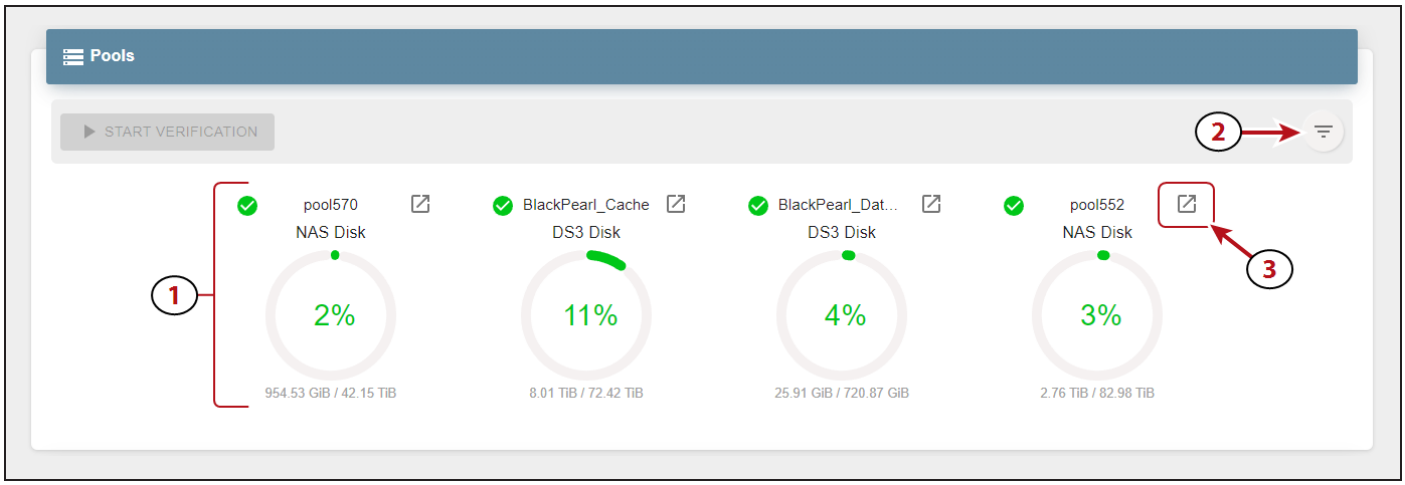


Figure 137 The Pools pane.

1. Each percentage graph displays both the used and remaining space for the associated pool.
2. Use the **Filter** button to select which pools to display on the Pools pane.
3. Click the **Details** button to view additional information about a specified pool.

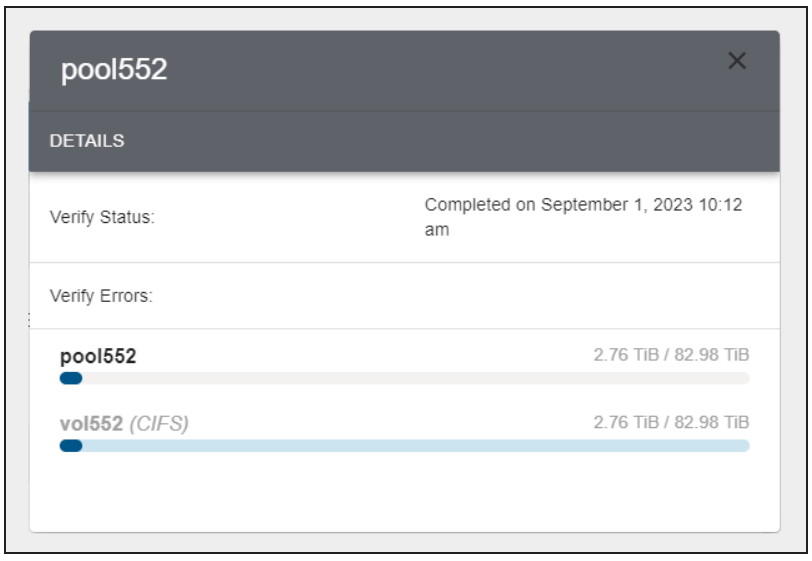


Figure 138 The pool details dialog box.

Use the **Start Verification** button to verify the data contained on the pool. See Start a Storage Pool Verification on page 266 for more information.

View Volumes

The Volumes pane displays information about all volumes configured on the BlackPearl system.

Note: The Volumes pane only displays on NAS systems.

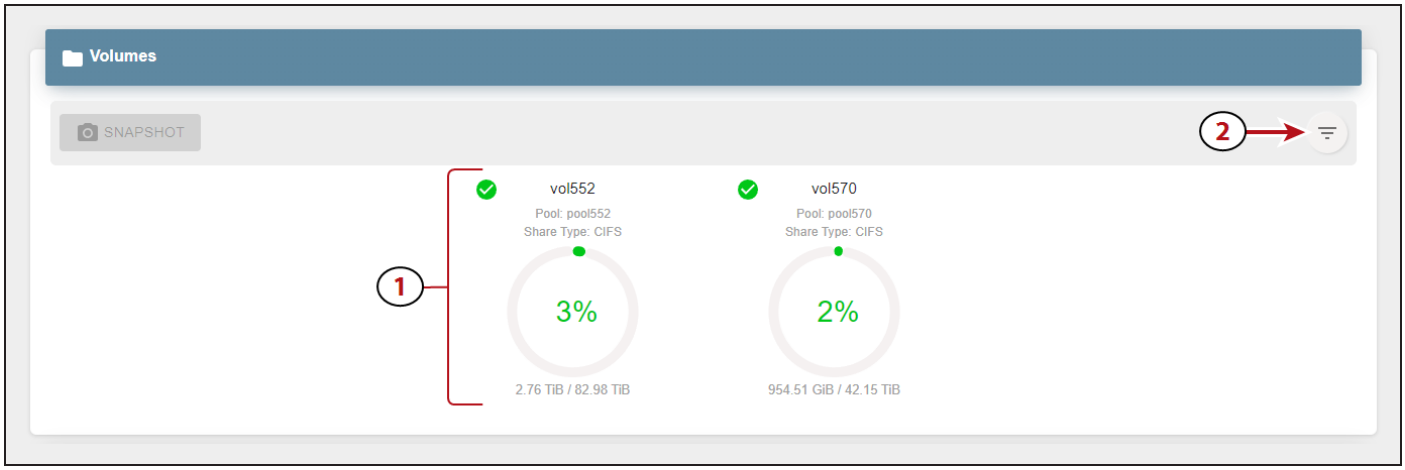


Figure 139 The Volumes pane.

1. Each percentage graph displays both the used and remaining space for the associated pool.
2. Use the **filter button** to select which pools to display on the Pools pane.

Use the **Snapshot** button to create a snapshot. For more information see Create a Volume Snapshot on page 263.

View Tape Partitions - Main View

The Tape Partitions pane displays information about the tape partitions configured on the tape library attached to the BlackPearl system. The Tape Partitions pane features both a main view and a tape cartridge state view.

To display the main view, manipulate the slider (**2**) to the left position.

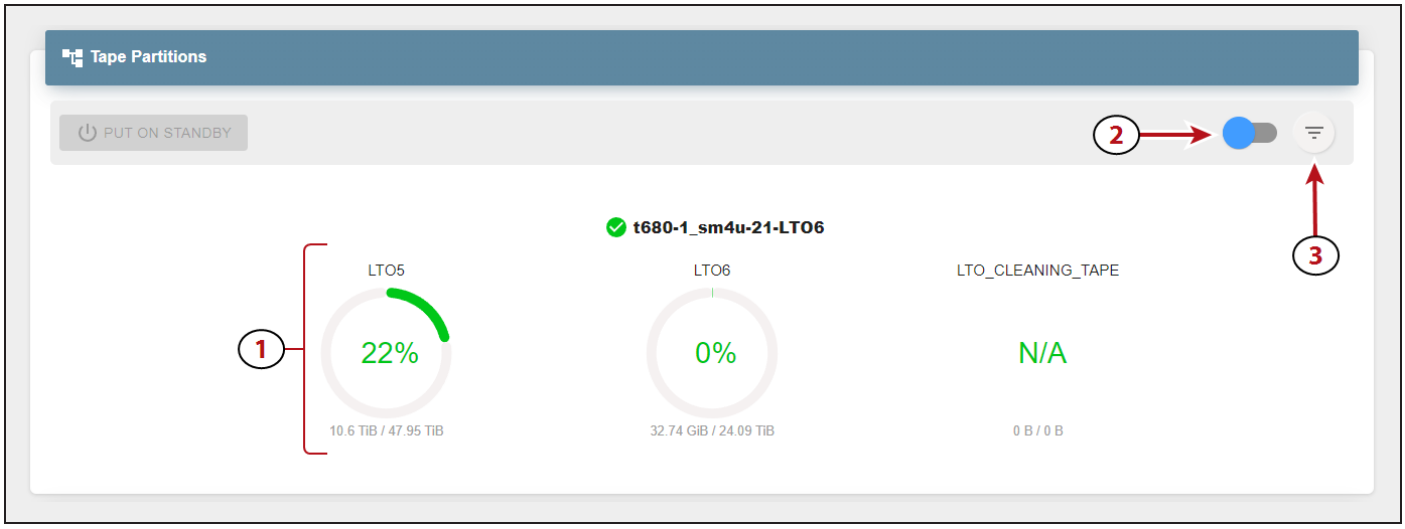


Figure 140 The Tape Partitions pane - main view.

1. Each percentage graph displays both the used and remaining space for the associated type and generation of media present in the tape partition. Mouse-over the green section of any percentage graph to display the amount of used space, and over the gray section to display the amount of remaining space.
2. Use the slider to change the display a graph of the current state of each tape cartridge present in the partition.
3. Use the **Filter** button to select which pools to display on the Tape Partitions pane.

If you need to service the tape library, you can put a tape partition into a standby state. See Put a Tape Partition into Standby on page 266 for more information.

View Tape Partitions - Tape State View

The Tape Partitions pane displays information about the tape partitions configured on the tape library attached to the BlackPearl system. The Tape Partitions pane features both a main view and a tape cartridge state view.

To display the tape cartridge state view, manipulate the slider (**2**) to the right position.

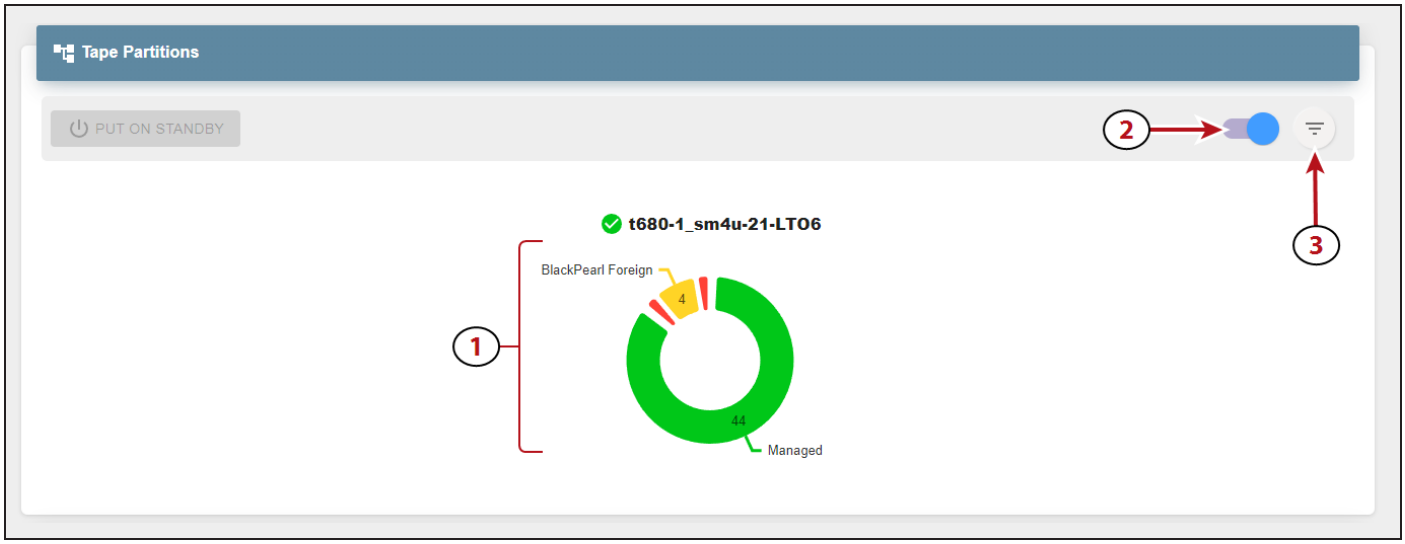


Figure 141 The Tape Partitions pane - main view.

1. The state of all tape cartridges in the partition. Each state combines different generations of tape media if present. Mouse-over any part of the graph to display more detailed information.
2. Use the slider to change the display a graph of the current state of each tape cartridge present in the partition.
3. Use the **Filter** button to select which pools to display on the Tape Partitions pane.

If you need to service the tape library, you can put a tape partition into a standby state. See Put a Tape Partition into Standby on page 266 for more information.

View Tape Drives

The Tape Drives pane displays information about all tape drives installed in the tape library connected to the BlackPearl system.

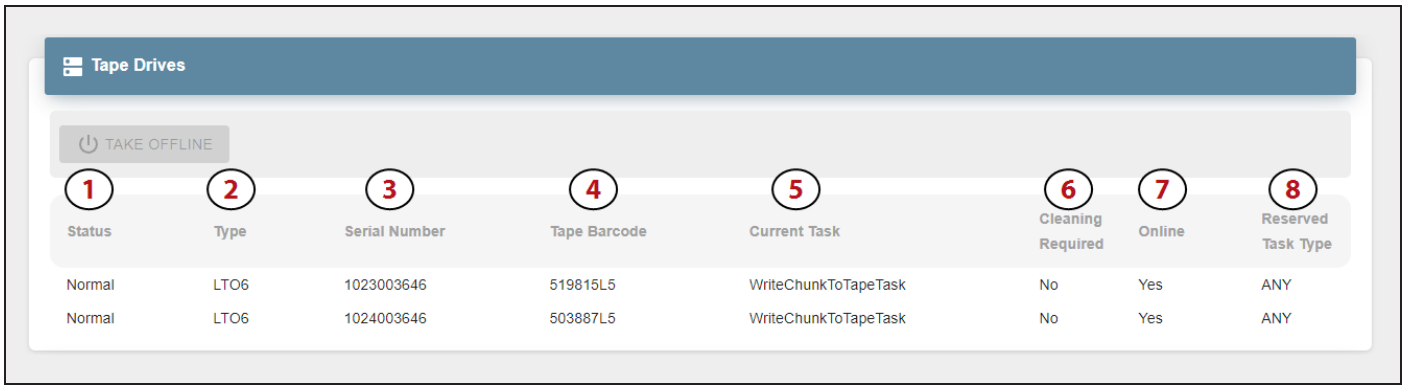


Figure 142 The Tape Drives pane.

1. The current status of the tape drive.
2. The drive type and generation.
3. The drive serial number as assigned by the tape library.
4. The physical barcode of the tape cartridge loaded into the tape drive. This field is blank when no tape is loaded.
5. The current task being performed by the drive. This field is blank when no task is in progress.
6. Indicates if the tape drive requires cleaning.
7. Indicates if the tape drive is online or offline.
8. The reserved task type, if configured. The default setting is Any.

Use the **Take Offline** button to take the drive offline. See Offline a Tape Drive on page 266 for more information.

View Tape Management

The Tape Management pane displays the status of all managed tapes in the tape library connected to the BlackPearl system.

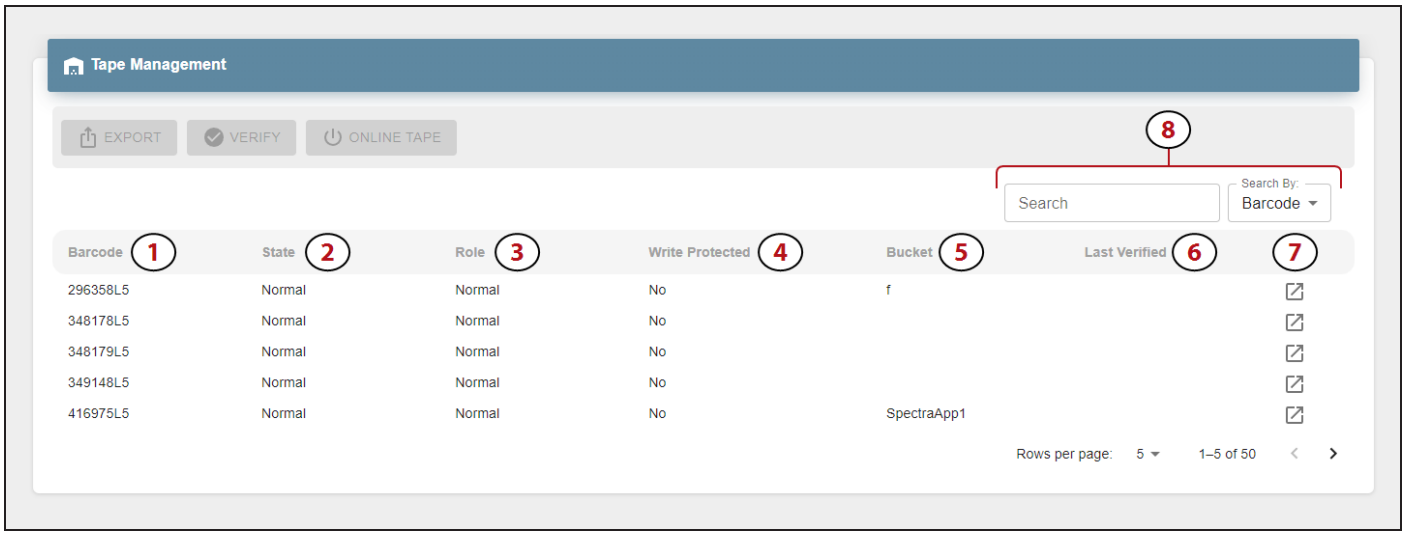


Figure 143 The Tape Management pane.

1. The physical barcode label on the tape cartridge.
2. The current state of the tape cartridge. See the *BlackPearl User Guide* for more information.
3. Indicates if the tape is configured for use as a **Normal** or **Test** tape.
4. The physical **Write Protected** status of the tape cartridge.
5. The name of any BlackPearl bucket(s) present on the tape cartridge.
6. Displays the timestamp of the last tape verification.
7. Click the **Details** button to display additional information about the selected tape cartridge.
8. Use the **Search** entry field and **Search By** drop-down menu to find a specific tape cartridge.

See one of the following sections for instructions to export, verify, or online a tape cartridge:

- Export a Tape Cartridge on the next page
- Verify a Tape Cartridge on page 264
- Online a Tape Cartridge on page 264

DASHBOARD ACTIONS

In addition to displaying information about the BlackPearl system, the embedded dashboard allows you to perform the most frequently-used actions as described in the sections below.

Create a Volume Snapshot

A volume snapshot is an image of a volume's configuration and data makeup as they were when the snapshot was generated. Restoring to a previously created snapshot allows you to go "back in time" and restore the volume to the state it was in when the snapshot was created.

Here is how to create a volume snapshot:

1. In the BlackPearl dashboard, navigate to the **Volumes** pane.

   Note: The Volumes pane only displays on NAS systems.

2. **Select** the volume for which you want to create a snapshot.
3. Click **Snapshot**.
4. If desired, edit the pre-generated **Snapshot** name.

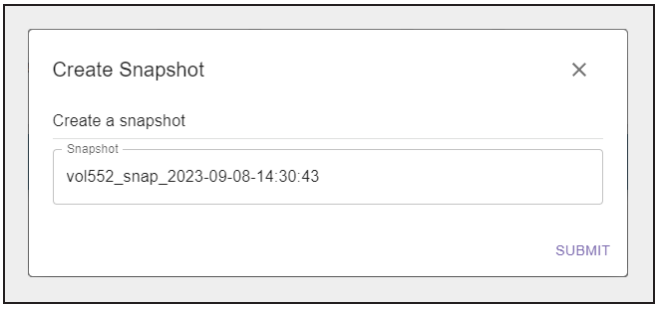


Figure 144 The Export Tape dialog box.

5. Click **Submit**.

Export a Tape Cartridge

Exporting a tape cartridge prepares it for physical removal from the attached tape library. In a Spectra Logic tape library, the cartridge is moved from the storage pool to the Entry/Exit pool, before it is physically exported from the library at the library front panel.

1. In the BlackPearl dashboard, navigate to the **Tape Management** pane.
2. **Select** the tape you want to export.
3. Click **Export**.

4. If desired, edit the **Export Label** and **Export Location**.

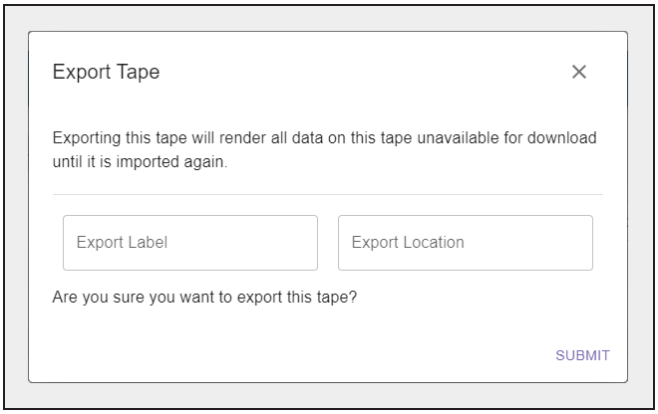


Figure 145 The Export Tape dialog box.

5. Click **Submit**.

Online a Tape Cartridge

Setting a tape cartridge to "online" prepares the cartridge for use by the BlackPearl system. This allows the system to use the tape cartridge for data storage operations.

Here is how to online a tape cartridge:

1. In the BlackPearl dashboard, navigate to **Tape Management**.
2. Select a tape in the **Offline** state.
3. Click **Online Tape**.
4. Click **Submit**.

Verify a Tape Cartridge

The BlackPearl system can perform a data integrity verification of all data on a selected tape cartridge to confirm it is still viable. While the verification is in progress, client access has priority over the data integrity scan.

Here is how to verify a tape cartridge:

1. In the BlackPearl dashboard, navigate to **Tape Management**.
2. **Select** the tape you want to verify.
3. Click **Verify Tape**.
4. Click **Submit**.

Change Job Priority

If desired, you can change the priority of an active job on the BlackPearl system.

Here is how you change the priority of a job:

1. In the BlackPearl dashboard, navigate to the **Jobs** pane.
2. If necessary, click **Active** to display the list of active jobs.
3. **Select** the job for which you want to change priority.
4. Use the **drop-down** menu to select a new priority for the job.
5. Click **Submit**.

Create a Bucket

Buckets on the BlackPearl system are data transfer targets for read and write operations. When you create a new bucket on the solution, you assign it a owner and a data policy. You can then use the new bucket in your other Spectra software applications as a target for data storage on the BlackPearl solution.

Here is how you create a new bucket:

1. In the BlackPearl dashboard, navigate to the **Buckets** pane.
2. Click **Create**.
3. Enter a **Bucket Name**.

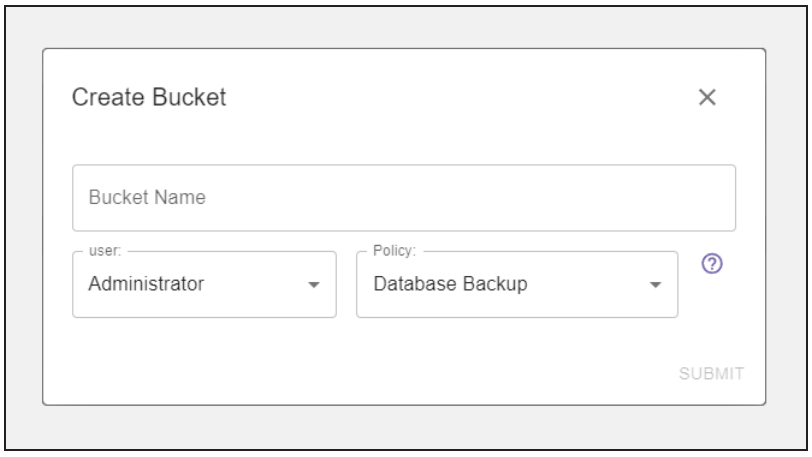


Figure 146 The Create Bucket dialog box.

4. Using the **User** drop-down menu, select an owner for the bucket.
5. Using the **Policy** drop-down menu, select a data policy for the bucket.
6. Click **Submit**.

Start a Storage Pool Verification

The BlackPearl system can perform a data integrity verification of all data on a selected storage pool to confirm it is still viable.

Here is how to start data verification on a storage pool:

1. In the BlackPearl dashboard, navigate to the **Pools** pane.
2. **Select** the pool that you want to verify.
3. Click **Start Verification**.
4. Click **Submit**.

Put a Tape Partition into Standby

If you need to perform service on the tape library associated with your BlackPearl gateway, or with the BlackPearl gateway itself, you must first put the tape library into a standby state. Otherwise, the BlackPearl gateway may attempt to use the tape library while it is in service.

Note: After the tape partition is placed in standby, any currently running tape operations continue until they are complete, which may take 30 minutes or longer.

Here is how to out a tape partition into standby:

1. In the BlackPearl dashboard, navigate to the Tape Partitions pane.
2. Select the partition you want to set to standby.
3. Click **Put On Standby**.
4. Click **Submit**.

Offline a Tape Drive

If a tape drive is experiencing errors and needs to be physically replaced, the drive can be taken offline to prevent the BlackPearl system from using the drive for data storage operations until the replacement is complete.

Here is how to offline a tape drive:

1. In the BlackPearl dashboard, navigate to the **Tape Drives** pane.
2. **Select** the drive you want to offline.
3. Click **Take Offline**.
4. Click **Submit**.

Chapter 13 - Troubleshooting

The first step in troubleshooting StorCycle solution errors is to review any System Messages that have been posted by the StorCycle solution (see System Messages on page 239) and take any action described in the message(s). The sections below provide additional troubleshooting information.

ACCESSING THE SUPPORT PORTAL

The Spectra Logic Technical Support portal provides access to the Knowledge Base, the current version of BlueVision software for the library, drive firmware, drive device drivers, and additional service and support tools. You can also open or update a support incident.

Create an Account

Access to User Guides and compatibility matrices does not require you to create an account. You must create a user account and log in to access Release Notes or repair documents, to download the latest version of BlueVision software, or to open a support incident.

1. Access the Technical Support portal login page at *support.spectralogic.com*.
2. On the home page, click **Register Now**.

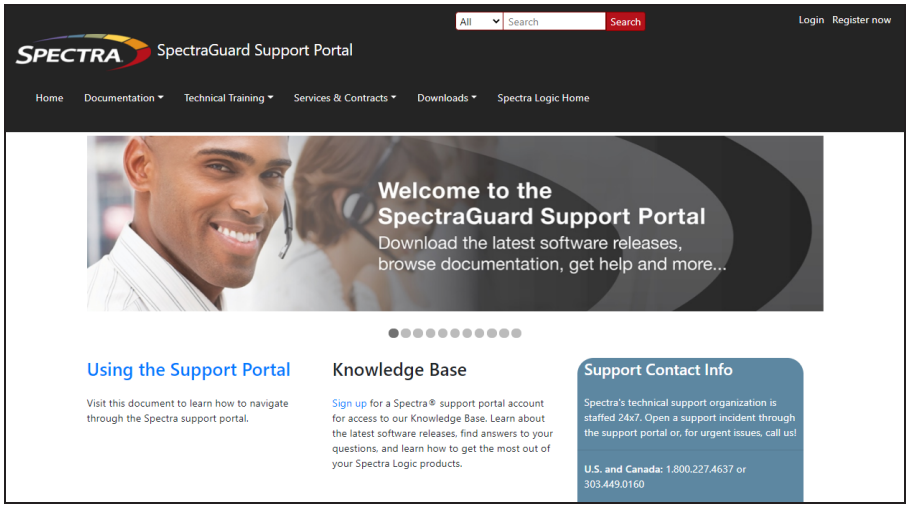


Figure 147 The Spectra Logic Technical Support portal home page.

3. Enter your registration information. Your account is automatically associated with the serial numbers of all Spectra Logic products owned by your site.
    - If you have an invitation, follow the link and enter the invitation code

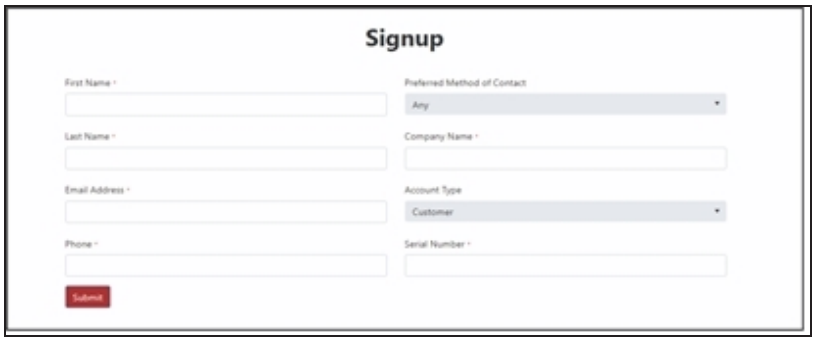


Figure 148 The Signup screen.

    - If you do not have an invitation, enter the requested information to create your account. When you are finished, click **Submit**.

When the account is approved, you receive an email with an initial password. Use your email address and the password provided in the email to log in to your account. After you log in, you can change your password if desired.

Log Into the Portal

Use your email address and password to log into the Technical Support Portal.

OPENING A SUPPORT TICKET

You can open a support incident using the Spectra Logic Technical Support portal or telephone.

- Use the following instructions to open a support incident through the portal, or skip to Contact Spectra Logic Technical Support by Phone

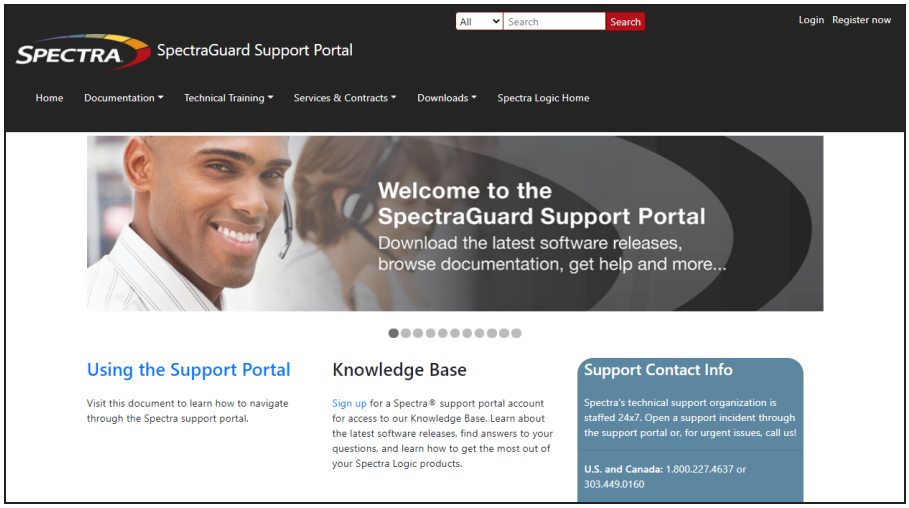


Figure 149 The Spectra Logic Technical Support portal home page.

1. Make notes about the problem, including what happened just before the problem occurred.
2. Gather the following information:
    - Your Spectra Logic customer number
    - Company name, contact name, phone number, and email address
    - The library serial number
    - Type of host system being used
    - Type and version of host operation systems being used
    - Type and version of host storage management software being used
3. If necessary, log in to the Support Portal by clicking **Login**, enter your **email address** and **password**, and click **Log In**.

4. Submit a support incident. Use the following instructions to search for help before submitting a ticket, or skip to Submit an Incident Directly.

   a. From any page, selected **Incident > Incidents & Inventory**.

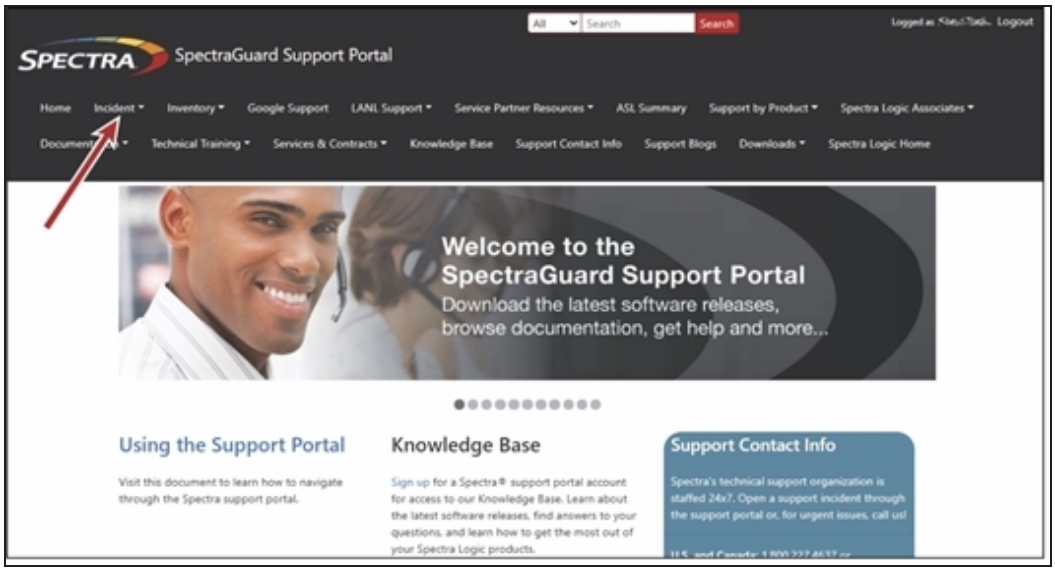


Figure 150 Select**Incidents>Incidents & Inventory**.

   b. Select **Open or View Incidents**.

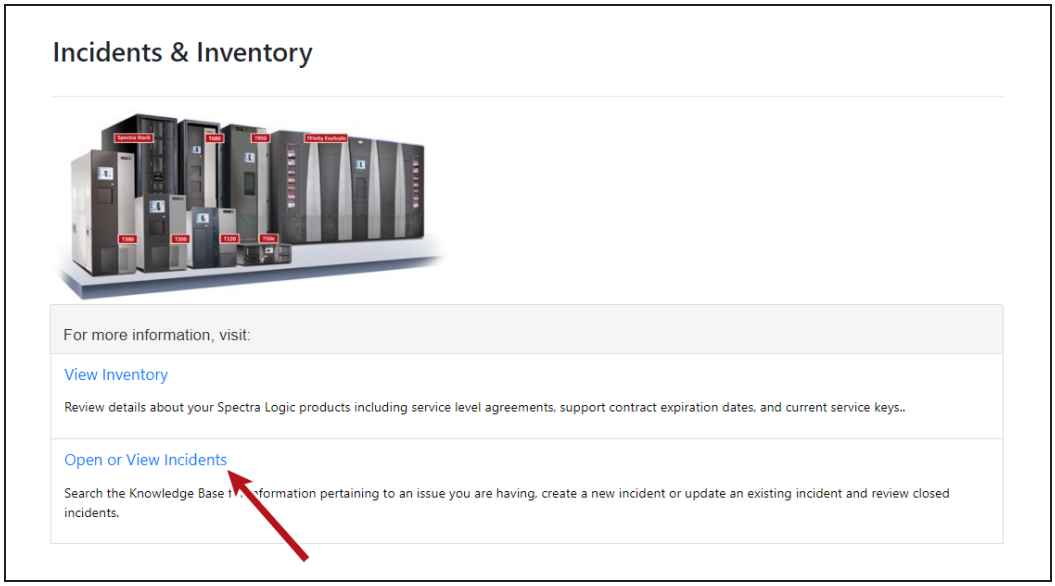


Figure 151 Select **Open or View Incidents**.

c. In the Search dialog box, enter a term or phrase about your problem (1) and click **Search** (2).

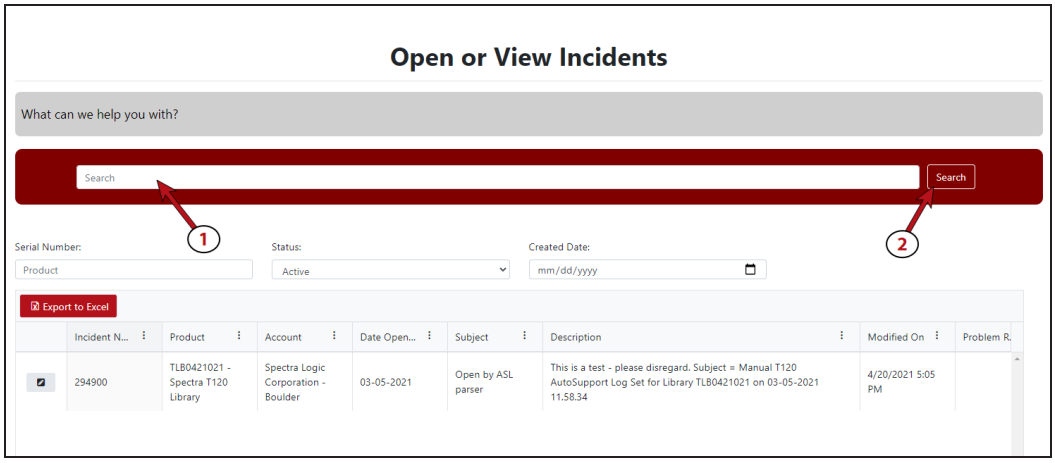


Figure 152 Enter a search phrase and click **Search**.

d. If the search does not provide an answer, click **Open a New Incident.**

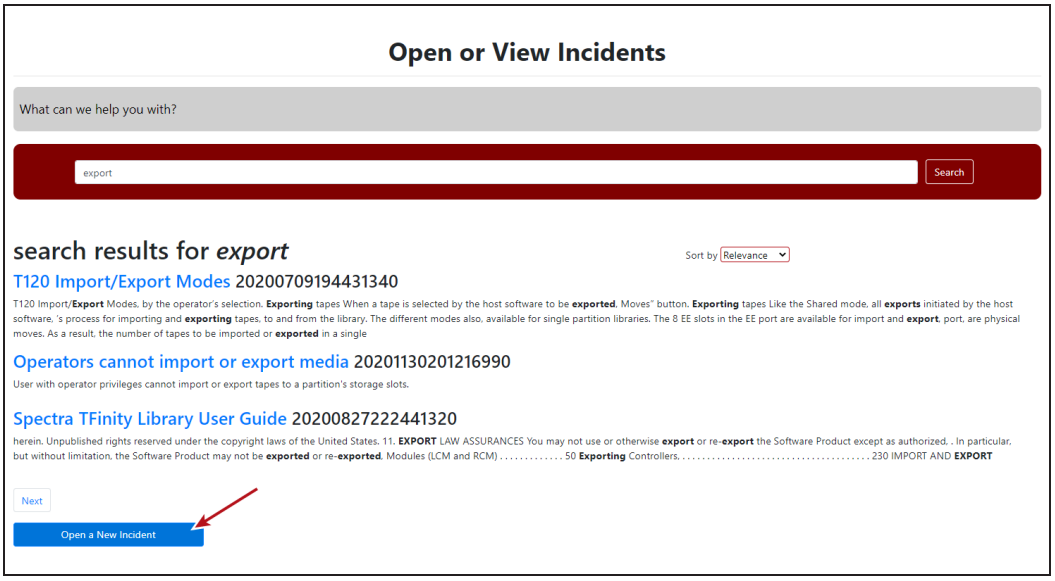


Figure 153 Click **Open a New Incident**.

e. Continue with Step 5.

- Submit an Incident Directly

  i. From any page, select **Inventory>My Inventory**.

  ii. Locate the row of the product for which you want to submit an incident and click **Create Incident**.

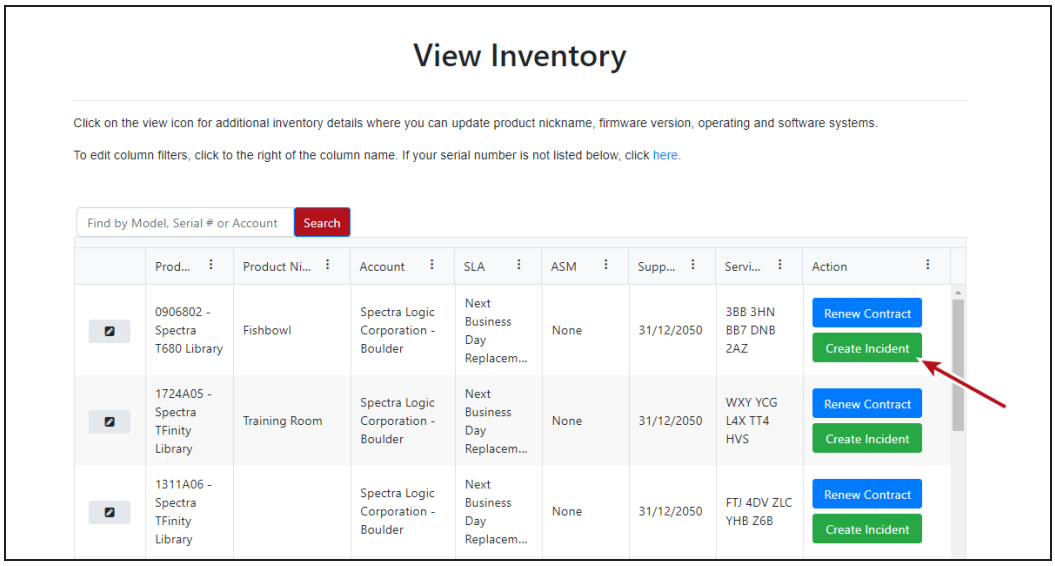


Figure 154 Click **Create Incident**.

  iii. Continue with Step 5 on page 273.

5. On the Create Incident page, enter the requested information providing as much detail as possible. When you are finished, click **Submit**.

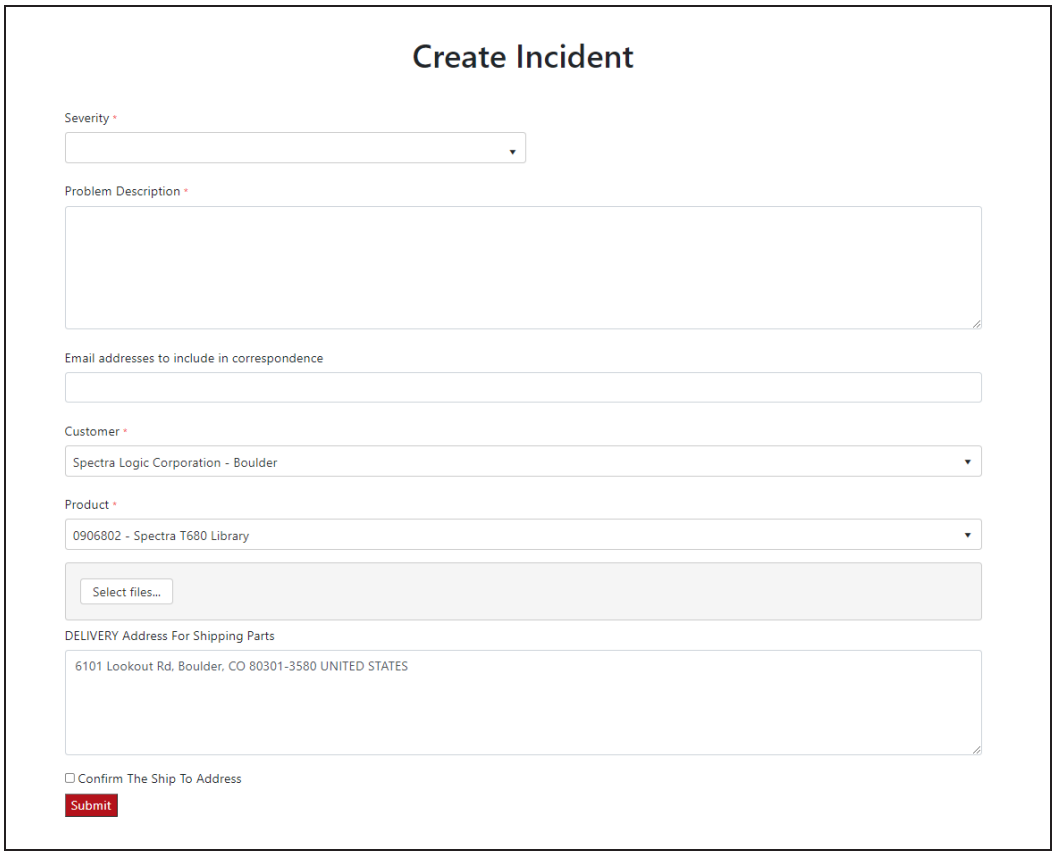


Figure 155 Enter information about your incident and click **Submit**.

- If you have multiple libraries and need to determine the serial numbers of the affected library.
- If the serial number of the affected library is not listed, contact Technical Support.

Resolving Configuration Issues

This section provides information about potential configuration issues you may encounter.

Issue	Cause / Solution
The StorCycle solution does not send email restore requests to the Administrator or messages to users as configured.	• SMTP must be configured for the StorCycle solution to send emails. See Configure SMTP on page 147. • To use the **Send Request to Administrator** HTML links, an email address must be configured for the Administrator user.
Changing the method used to determine the file age does not update scan data.	Changing this setting only affects future scans. You should rescan storage locations after making the change to update values in the database.
The session timed out in the middle of a task after extending the session timeout.	Changing the session timeout value does not extend the current session. The new session timeout setting takes effect the next time you login. **Note:** The User Interface timeout does not affect any jobs that are running.
After five unsuccessful login attempts, a local user is locked out.	The password must be reset by an administrator. See Reset a Local User Password on page 224 for instructions.
The StorCycle solution does not have access to all of the shares on the server.	The user running the StorCycle service must be able to access and have permission to read and write on all of the storage locations in the StorCycle environment. See Configure the User Account on page 46 for details.

Microsoft Windows Specific Issues

Issue	Cause / Solution
The StorCycle solution does not send email restore requests to the Administrator or messages to users as configured.	• SMTP must be configured for the StorCycle solution to send emails. See Configure SMTP on page 147. • To use the **Send Request to Administrator** HTML links, an email address must be configured for the Administrator user.

Issue	Cause / Solution
Active directory users get access denied errors even though **Allow any Active Directory /LDAP user to restore** is enabled (see Configure Active Directory / LDAP on page 137).	The StorCycle solution uses the domains configured on the server, including multiple / trusted domains, to access a DNS (Domain Name System) to resolve UNC (Universal Naming Convention) paths over the domain, and uses Active Directory to verify restore only users are valid on the domain. Configure the domain(s) on the server as needed.
If you install the StorCycle solution in one directory, remove it, and then install it in another directory, the program fails to run.	Uninstall the StorCycle solution, delete the ssc.yml file in the C:\ProgramData\Spectra Logic Corporation\Spectra StorCycle\config directory and re-install the StorCycle solution in the new directory.
The StorCycle user interface displays blank pages or tables.	This can be caused by the MongoDB service not running. To start the MongoDB service, do the following: **1.** Use the keyboard shortcut Windows logo key+R to open the Run window. **2.** In the **Open:** field enter `control admintools` and click **OK**. The Administrative Tools dialog box displays. **3.** Select **Services**. The Services dialog box displays. **4.** Locate the MongoDB service. If it is not running, right-click it and select **Start**.

Resolving Scan, Migrate / Store, Restore, and Database Backup Project Issues

Issue	Cause / Solution
The StorCycle solution says that a project name "already exists", but the project name does not display in any project lists.	Even after deleting a project, the StorCycle solution must maintain the history of any associated jobs to a project. Once a project has been used in some manner that name cannot be reused even if deleted. **Note:** This issue no longer applies to StorCycle 3.7 and later versions. Project names can be reused when all files are deleted from a project, and the project itself is deleted.
A BlackPearl storage location does not display as a source for scans or migrate / store projects.	Currently, only a BlackPearl NAS system, or BlackPearl S3 system can be configured as a source location. A BlackPearl Nearline Gateway cannot be configured as a source storage location.
Peak hour restrictions do not take effect at the scheduled times.	The time range is in Coordinated Universal Time (UTC), not local time.

Not all of the expected objects in a migrate / store project are migrated / stored.	• If **Use Last Scan** is selected:
	  • Only files present in the directory when the prior scan executed are considered for migration. Files added after the last scan are not considered.
	  • The current size and age of the file are considered against the selection criteria when determining files to migrate / store.
	• The StorCycle solution **does not** migrate files that have been previously migrated, even if the file has changed on the source storage device. If you want to archive the file again, you must first move it to another path location.
	Note: Starting with StorCycle 3.7, if versioning is enabled, the StorCycle solution **does** migrate / store files that were previously migrated / stored that have changed.
	• If a project attempts to migrate / store a file to a location in which a file of the same name already exists, the job fails. The existing file is not overwritten.
	• When a migrate / store job is canceled, the StorCycle solution leaves the job in whatever completion state it was in when the job cancellation command was received. No rollback occurs.

Issue	Cause / Solution
Not all expected objects in a restore project are restored.	• If a project attempts to restore a file to a location in which a file of the same name already exists, the job fails. The existing file is not overwritten. • When a restore job is canceled, the StorCycle solution leaves the job in whatever completion state it was in when the job cancellation command was received. No rollback occurs.
The StorCycle solution does not migrate / store all of the files meeting either the **Object Age** or **Object Size** criteria.	Only those objects meeting the **Object Age** and the **Object Size** requirements are included.
The StorCycle solution did not remove / replace all of the files that were migrated / stored.	When a migrate / store project is configured to delete the source file, or replace the source file with an HTML or symbolic link, the StorCycle solution checks the file timestamp and size to ensure that the file has not changed between the time it was migrated / stored and when it is deleted or replaced. If the file changed during this time, then the file is not deleted or replaced from the source storage, and a note is added to the job logs.
In a Windows Isilon environment, accessing a file using a symbolic link returns, "The request is not supported."	If you can create symbolic links on the Isilon share using a drive letter but not with a UNC path, then open a Command Prompt and run `gpupdate /force`.
HTML links replacing migrated / stored files include an IP address.	If the network does not support reverse DNS lookups, then the IP address of the storage location is used in the HTML link created during a migrate / store job.
When files are migrated / stored to a BlackPearl storage location configured to use packing and the zip file is downloaded from the BlackPearl system directly using the Eon Browser or a BlackPearl client, double-clicking the zip file does not open a directory with the individual files.	Using 7-zip or another non-OS-native zip application is necessary to extract the files.
A scan, migrate / store, or restore job fails with an error of “working directories are not siblings”.	A job using the same storage location branch is already in progress. Wait for the original job to complete and try the second job again.

Issue	Cause / Solution
A canceled migrate / store job stays in a “canceling” state.	If you cancel a migrate / store job that uses a BlackPearl system as the target, and the final storage target of the BlackPearl data policy is offline or unavailable, the job stays in a “canceling” state until the final storage target is back online so that the data in process can persist to the final storage target.
Recurring schedules are running an hour earlier or later than expected.	Daylights savings time is not handled by the solution, the server time is in UTC. So a scheduled job runs an hour earlier or later in local time than the original scheduled time depending on the time of year.
Limit Transfers During Peak Hours does not limit some transfers.	Limiting transfer during peak hours only applies when reading from the storage location. If the Storage Location Type is Source, this occurs when the location is scanned or is the source of a migrate / store project. If the Storage Location Type is Target, this occurs when a restore is done of a file previously migrated / stored to the target.
The permissions / ACLs on a directory changed after a restore.	When the StorCycle solution migrates / stores or restores files, it also migrates / stores or restores associated directories. While the StorCycle solution ensures that a file does not already exist on the target and does not overwrite the file, it may overwrite existing directories. When it overwrites the directory: • The Windows version of the StorCycle solution resets the permissions / ACLs based on the permissions / ACLs that are on the directory that it is migrating. • The Linux version of the StorCycle solution does not reset the permissions / ACLs (because Linux does not have an "Auto Inherit" flag like Windows).
Migrations were working, but then stopped working.	Check password expiration on the user running the StorCycle service.
If a migrate / store job with the Replacement Option **Remove Source File: create Symbolic link** or **Remove Source File: create HTML link** fails during post processing, an inconsistent state of deleted source files and created links may be present.	*After confirming the files are successfully migrated / stored*, delete the remaining source files and link files from the source manually, and then regenerate HTML links by creating a restore project and selecting **Restore HTML Links Only**. See Restore Wizard—Restore To on page 200 for more information. It is not possible to create a restore project to restore symbolic links.

Issue	Cause / Solution
With StorCycle running on a Windows server, files are inheriting rights from the directory instead of keeping the files rights.	The user running the StorCycle service does not have the take ownership rights required. See Configure the User Account on page 46 for instructions.
With StorCycle running on a Windows server, System Access Control Lists (SACLs) are not retained when the StorCycle solution migrates / stores Windows system files.	For Windows system files and CIFS files shares, the StorCycle solution migrate / stores and restores file permissions / ACLs, but does not migrate / store Alternative Data Streams or SACLs.
With StorCycle running a Windows server, the StorCycle solution displays the error "The process cannot access the file because it is being used by another process".	Having the target directory for a migrate / store job or the restore destination for a restore job open in Windows Explorer can cause this error. Close Windows Explorer and try the job again.
Logs roll frequently on a Linux installation.	When SELinux is enabled, mongod is prevented from accessing the files “netstat” and “snmp” by default. This causes warnings to be generated and saved in /var/log/messages and can cause that log to roll frequently. See the warnings in the logs to address those problems if desired.
Running multiple concurrent restores from the same Microsoft Azure Archive job can complete with errors and not restore all files due to an Azure error "409: This operation is not permitted on an archived blob".	Do not run concurrent restores from the same Microsoft Azure Archive job.
A restore fails with the warning “This security ID may not be assigned as the owner of this object."	The user recorded as the owner of the files during the migrate / store does not have permission to be assigned as the owner upon restore. See *https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc978898(v=technet.10)* for more information.

File Transfer Failures

The StorCycle solution includes mechanisms to monitor file transfers. For cloud and BlackPearl targets, if there is a problem transferring a file, the StorCycle solution retries the file transfer several times before failing. For NAS targets, the file transfer fails after the first unsuccessful attempt. Whatever the target type – NAS, BlackPearl, or Cloud – if a file transfer fails, the file is marked as failed and the file failure is logged. The StorCycle solution then attempts to transfer the remaining files in the job. Similar error messages are grouped on the Job Details screen.

StorCycle Verification CLI Utility

The Verification CLI utility is used to check the current configuration of the StorCycle solution to a BlackPearl Nearline gateway. The utility can also be used to generate checksums of migrated files and directories for comparison to the checksums used by the StorCycle application.

IMPORTANT Spectra Logic recommends verifying the functionality of your StorCycle configuration after creating a BlackPearl storage target.

For access to the download location for the verification CLI utility, contact Spectra Logic Professional Services. You must unzip/unpack the file after downloading it.

Note: For a Windows installation, Spectra Logic recommends a directory under the parent directory C:\StorCycle\.

Full Verification Test

The utility creates a test file and moves the file to the BlackPearl system, and then to tape storage. The utility then requests the file and confirms it moves back to the BlackPearl system, and then to the original source storage. The utility generates checksums to confirm the file is unchanged.

This utility takes several minutes to complete, and takes longer on a busy/active BlackPearl system.

Use **ssc-cli.exe** in conjunction with the following parameters.

Parameter	Definition
command full_verify	The name of the command.
url <value>	The URL of the StorCycle host.
name <value>	The StorCycle Administrator username.
password <value>	The StorCycle Administrator password.
directory <value>	The directory to use for the verification test.
clone <value>	The name of the BlackPearl storage target configured in StorCycle.
endpoint <value>	The IP address of the BlackPearl management port.

Parameter	Definition
access_key <value>	The S3 access key of an administrator user on the BlackPearl system.
secret_key <value>	The secret key of an administrator user on the BlackPearl system.
ignore_cert (optional)	Use this parameter to ignore certificate errors when running the test.

Usage Example

$ ssc-cli --command full_verify --url https://localhost/openapi --name Administrator --password spectra --ignore_cert --directory C:\\StorCycle\\verify --clone bp-sandbox --endpoint http://10.85.41.36 --secret_key btkDKJBd --access_key k2dsn5 --ignore_cert

The console displays the progress of the test as it runs. The test passes successfully when **Verify succeeded** displays in the console. Confirm the two **checksums** match.

Generate Checksums

This utility is used to verify file checksums outside out SC to be compared to the Catalog File Listings in the StorCycle application. This utility can be used to verify the checksum of a single file, or a directory of files.

Use **ssc-cli.exe** in conjunction with the following parameters.

Parameter	Definition
command checksum_test_file or command directory_checksum	The name of the command. • Use **checksum_test_file** for a single file • Use **directory_checksum** for a directory of files.
filename <value>	The name of the file for which you want to generate a checksum. **Note:** This parameter is only included when running the **checksum_test_file** command.
directory <value>	The system path for the directory for which you want to generate checksums, or the system path for the single file specified in the **filename** parameter.

Parameter	Definition
out <value>	The name of a CSV file to generate containing the checksums of all files in the specified directory. **Note:** This parameter is only included when running the **directory_checksum** command.

Usage Example - Single File

$ ssc-cli --command checksum_test_file -file_name testfile220526083234.txt --directory C:\\StorCycle\\verify\\verify-test-source

Usage Example - Entire Directory

$ ssc-cli.exe --command directory_checksum --directory C:\\StorCycle\\shares\\two --out shares_two.csv

INDEX

E

F

G

I

J

L

M

N

O

P

R

S

T

U

W