Quest

Metalogix® StoragePoint 5.9.2

Hitachi HCP or HCAP Adapter Guide

© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Metalogix are trademarks and registered trademarks of Quest Software Inc. and its affiliates. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Metalogix® StoragePoint
Updated August 2020
Version 5.9

Contents

HCAP Adapter Configuration 4

HCP/HCAP Adapter Connection String Parameters 6

Example Storage Endpoint using HCP or HCAP Adapter 13

VerifyWrites 14

Retention Promotion from IMP 14

Event Based Retention 14

Appendix: Troubleshooting 15

Problem: Receive an error message when testing a storage profile. 15

Problem: Receiving errors on storage or retrieval of externalized content. 15

Problem: Newly uploaded content is not being archived as expected. 16

About Us 17

Contacting Quest 17

Technical Support Resources 17

1

HCAP Adapter Configuration

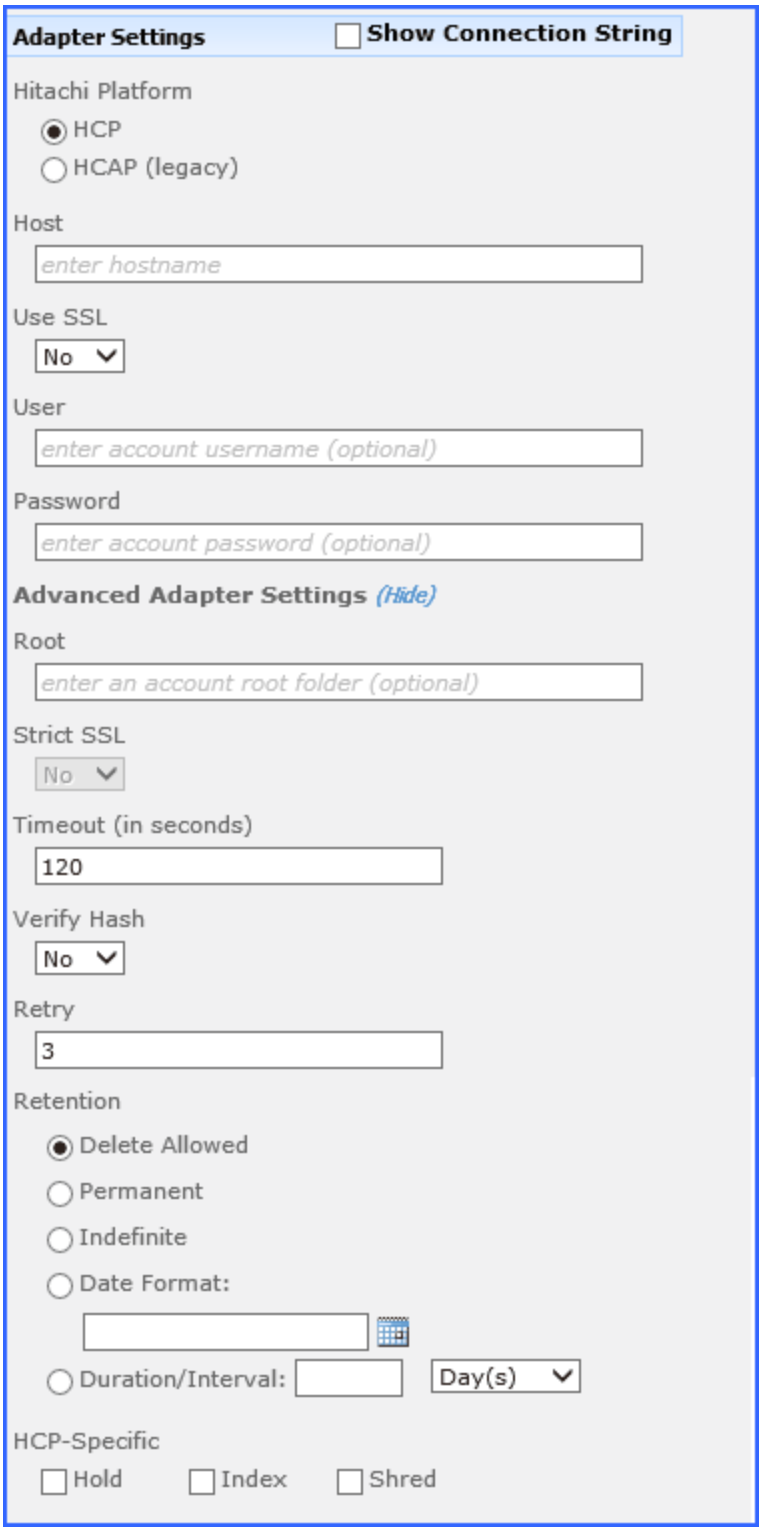
This section will provide you details on how to configure a storage endpoint's connection string to utilize the Hitachi Adapter. Please refer to the StoragePoint Reference Guide for information on managing Storage Endpoints.

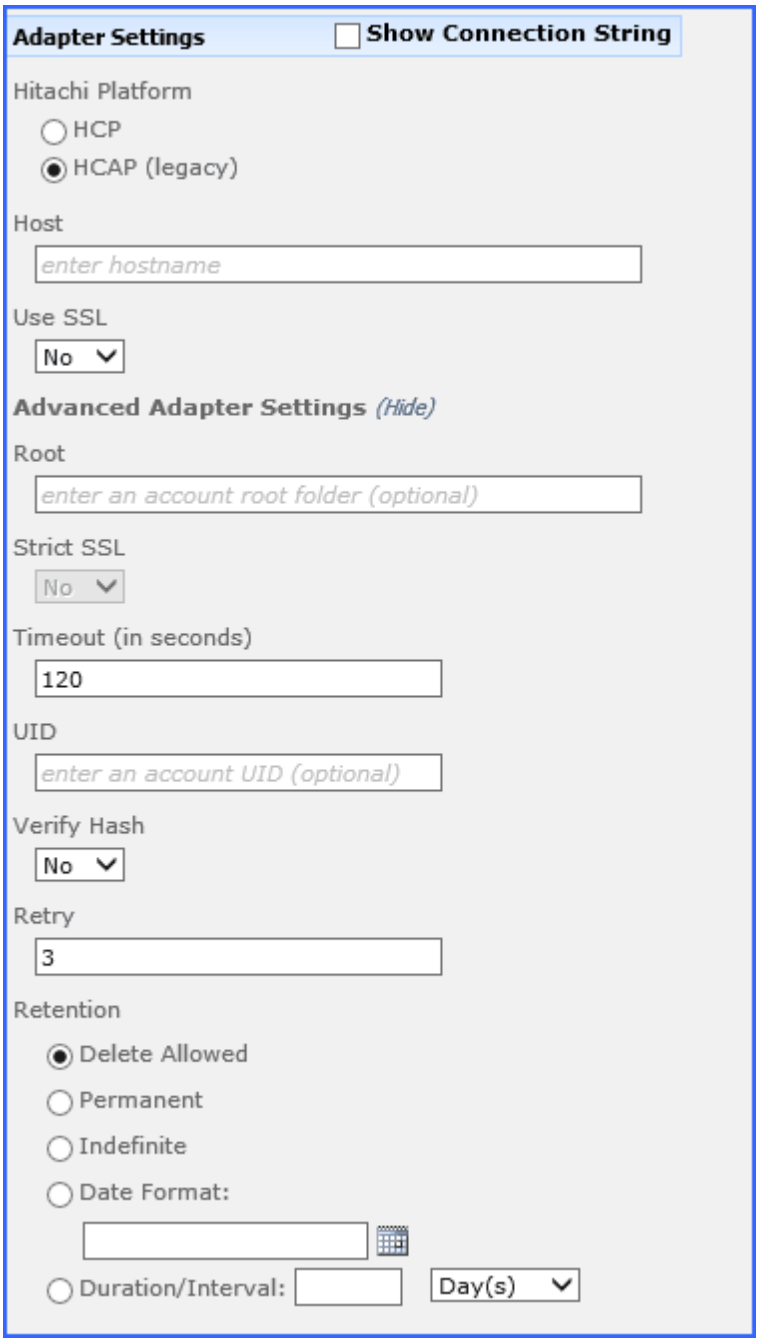
StoragePoint supports HCAP 5.x, HCP 6.x, HCP 7.x and HCP 8.x versions of the platform.

On the Application Management page, click *Storage and Backup Endpoints*.

Click *Create New Endpoint* or click the name of an existing storage endpoint that you want to edit.

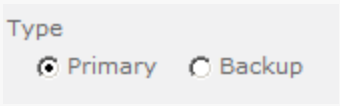
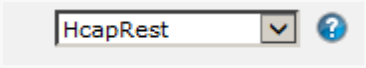
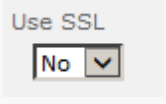
Select HCP or HCAP for legacy adapters. Click the *Show* link next to the Advanced Adapter Settings to see the additional fields.

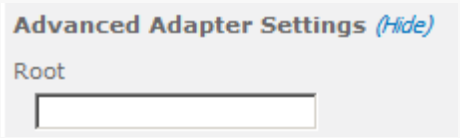
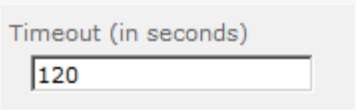

Adapter Settings
Show Connection String
Hitachi Platform
HCP
HCAP (legacy)
Host
enter hostname
Use SSL
No
User
enter account username (optional)
Password
enter account password (optional)
Advanced Adapter Settings (Hide)
Root
enter an account root folder (optional)
Strict SSL
No
Timeout (in seconds)
120
Verify Hash
No
Retry
3
Retention
Delete Allowed
Permanent
Indefinite
Date Format:
Duration/Interval:
Day(s)
HCP-Specific
Hold
Index
Shred

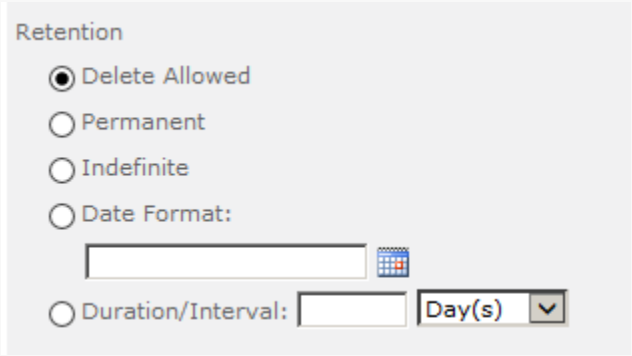


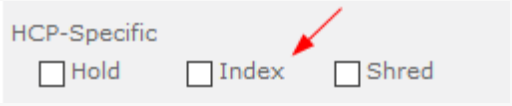
HCP/HCAP Adapter Connection String Parameters

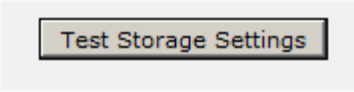
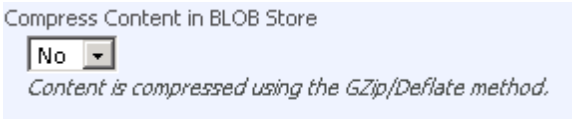
Setting	Value/Options
Name	Enter the unique name of the Storage or Backup Endpoint.

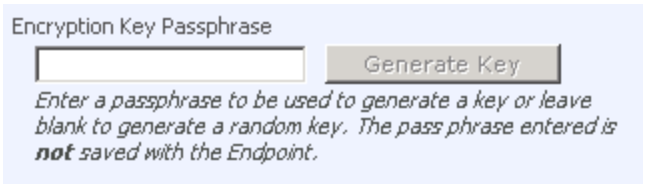
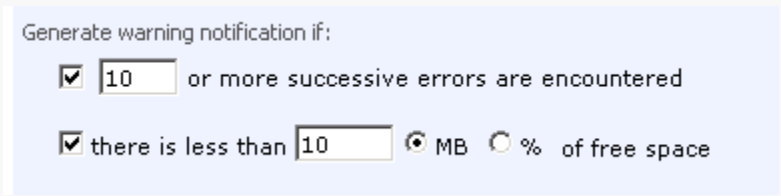
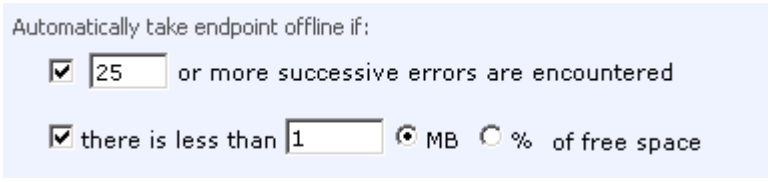
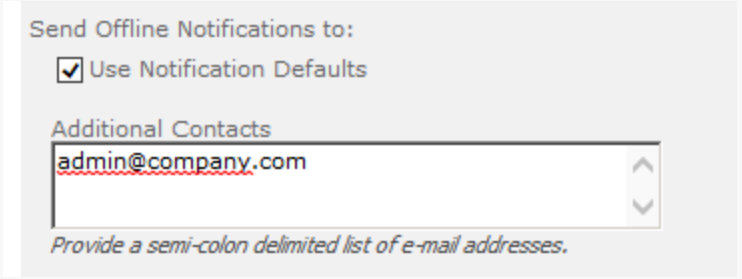
Setting	Value/Options
Type  See Backup Services Settings in the Reference Guide for more information on how Backup Endpoints are used.	*Primary* – this endpoint will be available for externalization when creating storage profiles. *Backup* – this endpoint will be in the Backup Services dropdown on the profile page. The selection is locked down when saving.
Status 	*Online* – Storage Endpoint should be available to associate to a Storage Profile and accept BLOBs. (default) *Offline (Read Only)* – A storage endpoint can be configured, but not made available for externalizing content. The BLOBs already on the endpoint are still read only.
 	Select the adapter for the endpoint that is being created.
 	Fully qualified domain name that represents the HCP tenant namespace, or if HCAP (legacy) system is used, fully qualified domain name or IP address that represents legacy HCAP system.
 	(*yes/no*) – Determines whether or not the adapter negotiates an SSL connection for all data (and metadata) transfers. Default = No.
 	User login and password used to access the HCP system. Not applicable for HCAP (legacy) system.

Setting	Value/Options
	This needs to be a local tenent to the HCP system and cannot be a domain account.
	Folder path to use when storing the SharePoint content under this profile. Facilitates the current best practice of dividing up the HCP/HCAP name-space by application. Please remember that HCP/HCAP paths and folder names are case sensitive.
	(*Yes/No*) If *UseSSL* is *Yes*, the *StrictSSL* flag controls whether or not the use of "self-issued" or otherwise suspicious certificates on the HCP/HCAP system will be tolerated. Note that the default certificate out of the box with HCP/HCAP is self-issued and will not work unless this flag is set to No (default).
	Number of seconds to wait for a response to any request before considering it an excessively long wait and raising an error condition. Default = 120.
	Identifies the "owner" of all content uploaded with this adapter. See HCAP documentation for details on UID, GID and permissions semantics. By default permission checking is disabled on HCAP (legacy) systems. Not applicable to HCP.

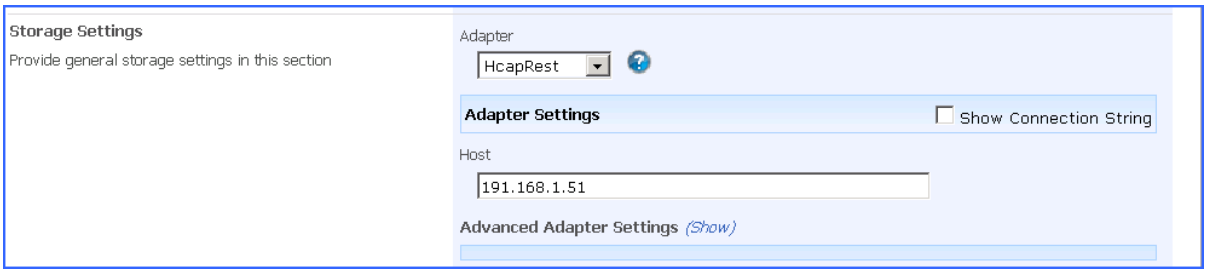
Setting	Value/Options
	(*Yes*/*No*) If set to *Yes*, adds content integrity checking by comparing a locally computed hash for the file bits against the hash returned from HCP/HCAP during upload operations. Default = No.
	Specifies the number of attempts to retry the network connection to HCP/HCAP before returning a failure result in case of network disruption or connectivity issues. Default = 3.
	If supplied, the HCP/HCAP adapter will calculate and supply a retention policy when saving content. Possible settings: Delete Allowed No special permissions are required to delete content on this endpoint. Permanent This maps to -1 or “Infinite retention, cannot be deleted” in HCP/HCAP. Indefinite This maps to -2 or “Initial Unspecified” in HCP/HCAP. Content cannot be deleted, but retention can be changed at a later time. Date Format

Setting	Value/Options
	This sets a date for the retention policy. Click the calendar icon to select a date, or type it like this example: 08/31/2009 Duration/Interval Type a number in the first box, and select an interval from the dropdown. The interval may be days (D), months (M) or years (Y). Example: 5D would equal 5 Days NOTE: You can NEVER shorten the retention period once it has been established, unless it was initially set to Indefinite.
	If Hold is set to true (checked) you can place an object on hold. An object that is on hold cannot be deleted, even by a privileged delete operation. Holding objects is particularly useful when the objects are needed for legal discovery.
	If Index is set to true (checked), the metadata query engine indexes custom metadata. Having index set to true will speed-up metadata search experience.
	If Shred is set to true (checked) all objects will be shredded when deleted. Shredding, also called secure deletion, is the process of

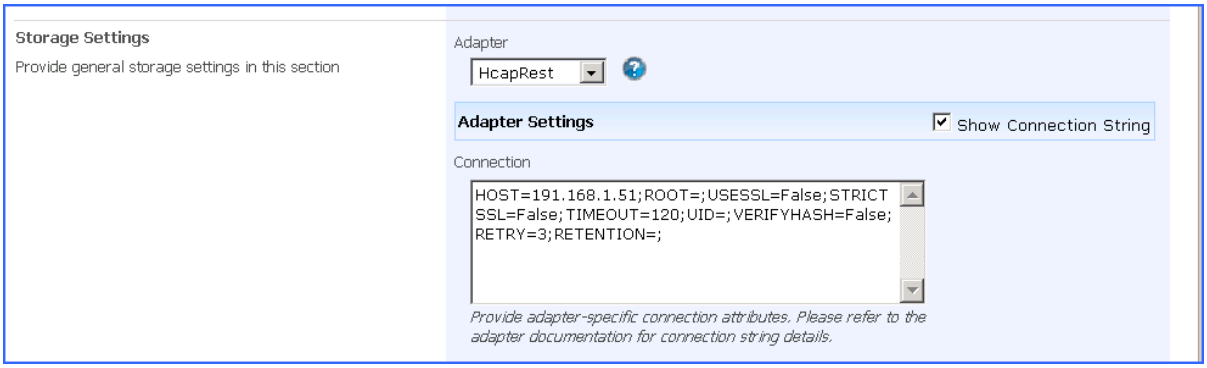
Setting	Value/Options
	deleting an object and overwriting the places where its copies were stored in such a way that none of its data or metadata, including custom metadata, can be reconstructed.
	If the endpoint is on a WORM (Write Once, Read Many) device, Unused BLOB Cleanup will ignore this endpoint.
	No – Externalized content BLOBs are not placed in folders. *Yes* – Externalized content BLOBs are placed in folders (default). If *Folder Content in BLOB Store* is *Yes* then you can select a date/time folder scheme from the dropdown. YYYY/MM/DD/HH/MM is the default.
	The Test Storage Settings button can be used at this point, or after completing the endpoint configuration, to verify that the endpoint is accessible.
	*No* – Externalized content BLOBs are not compressed (default). *Yes* – Externalized content BLOBs are compressed.
	None – Encryption will not be applied to externalized BLOBs (default).

Setting	Value/Options
	AES (128 bit) – 128 bit AES encryption will be applied to externalized BLOBs. *AES (256 bit)* – 256 bit AES encryption will be applied to externalized BLOBs.
	Enter a passphrase to use when generating the encryption key. Using a passphrase will help you re-create the encryption key if necessary. You can generate a random key by leaving the box blank and clicking the *Generate Key* button. The encryption key passphrase will be hidden.
	A warning email can be sent if it encounters errors.
	An online storage endpoint can be automatically taken offline if it encounters errors. If a storage endpoint is taken offline automatically, BLOBs that were intended to be written to that endpoint will go to the content database.
	Default email addresses for system error and offline notification can be entered. Check the box to include the list of Default Notification Contacts specified on the General Settings page.

Example Storage Endpoint using HCP or HCAP Adapter



Click the *Show Connection String* checkbox to edit the connection string. Otherwise, fill in the connection fields shown for the adapter selected. Notice that the connection string parameters are name/value pairs separated by semi-colons.



NOTE: Adapter parameters are not case-sensitive.

NOTE: Clicking the Test Storage Settings button on a storage profile using the HCP Adapter could result in an error. The profile test performs several operations, including a delete operation. If you are setting a retention parameter on the connection string then you will receive an error letting you know that the delete failed. This should not be considered a failure of the test.

NOTE: You should always use a passphrase when generating encryption keys. The passphrase gives you a means of re-creating keys should they become unrecoverable or corrupt. It is very important to remember or record the passphrase outside of Metalogix StoragePoint. Otherwise, encrypted content could become irretrievable in the event of a database failure.

If you choose to externalize content you should test the storage profile settings by clicking the *Test Storage Settings* button. A message under the button will indicate whether or not the test was successful. If the test fails the message will include the error that was the root cause of the failure.

NOTE: When testing access to an endpoint from within Central Administration, the Identity of the Application Pool hosting the Central Administration Site is the one that is being used for the test. If there are different Identities used for other Web Applications in the Farm then those identities will also need access but cannot be tested from within Central Admin itself. See BLOB Store Security and Metalogix StoragePoint Required Privileges in the Metalogix StoragePoint Reference Guide.

VerifyWrites

This option posts back to StoragePoint to validate that the BLOB was written to the endpoint. It is not part of the connection string by default, but can be added by editing the connection string only; there is no user interface for this option. If verbose logging is enabled, the logs may contain information such as 'Written file verified as present: <filename>.'

VERIFYWRITES=true;

Retention Promotion from IMP

If retention settings have been configured in the SharePoint site or library, those retention settings will stay with the BLOB when it goes to the endpoint. To enable this, there is a box on the endpoint screen, when adding the endpoint to the profile. If the profile already exists, with the endpoint added, the feature can still be enabled, but will only be applied to BLOBs created after the feature is enabled.

1. Open or create the profile.
2. Add the endpoint to the profile.
3. On the endpoint screen, at the bottom, will be an option to Enable Retention Promotion from IMP. Check this box.

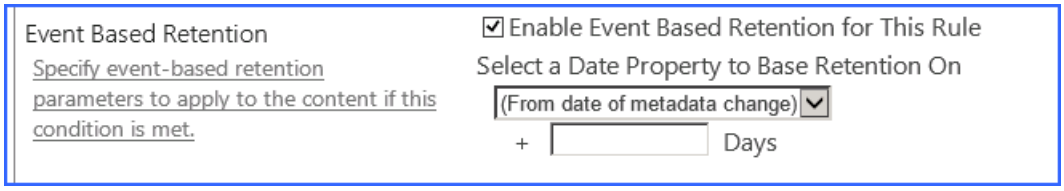
Event Based Retention

EBR is a feature that can be configured for certain storage endpoints. In addition to the default retention that can be configured on the endpoint, certain actions like updating a field can update the content to specify a different retention period. The steps for configuring the adapter to support EBR are outlined below.

The endpoint must be added to the profile for the following steps to work.

1. Expand the Archiving section of the profile.
2. Set the Enable Archiving dropdown to Yes.
3. Click New Rule.
4. Click Change to select the scope of the rule, which can be as wide as the profile scope or as narrow as a list. Click Ok.
5. Select Metadata Change Rule and click New Condition.
6. By selecting the same endpoint that was added to the profile, a new field displays for designating EBR. Check the EBR box, select a field to base the retention on, and enter the

number of days to which to update the retention time.



7. Click OK on the Condition window.
8. Click OK on the Rule window.
9. Click Save on the archiving page.
10. (OPTIONAL) Select Immediately or schedule a timer job to run, to process existing content for this archiving rule. Click OK on the Process Existing page.

NOTE: Content retention is modified when the field changes, not when it is uploaded. Uploaded content will receive the default retention setting, but modifying the designated EBR field will update the retention setting for that content.

Appendix: Troubleshooting

Problem: Receive an error message when testing a storage profile.

When clicking the *Test Storage Settings* button on a storage profile using the HCP or HCAP adapter you receive an error similar to this:

This error is because a RETENTION value was specified on the storage profile's Connection String and StoragePoint cannot delete the externalized test file. This should be considered a successful test.

Problem: Receiving errors on storage or retrieval of externalized content.

Wherever possible, StoragePoint surfaces error messages returned by HCP/HCAP either directly to the user or within the SharePoint ULS logs. You should refer to your HCP/HCAP documentation for errors logged by the HCP/HCAP Adapter.

Problem: Newly uploaded content is not being archived as expected.

For event based retention to work, the item has to exist before it can be tagged with retention during the archive process. So if content is uploaded with a change to the metadata that would normally archive the item, it won't be archived. However, any subsequent change to the item will flag it for archiving, and the next successful run of the content queue migrator will archive that content.

2

About Us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation

- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product