



# Hitachi Content Platform

## Managing a Tenant and Its Namespaces

© 2009–2015 Hitachi Data Systems Corporation. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Data Systems Corporation (hereinafter referred to as “Hitachi Data Systems”).

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document may not be currently available. Refer to the most recent product announcement or contact Hitachi Data Systems for information about feature and product availability.

**Notice:** Hitachi Data Systems products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems agreements. The use of Hitachi Data Systems products is governed by the terms of your agreements with Hitachi Data Systems.

By using this software, you agree that you are responsible for:

- a) Acquiring the relevant consents as may be required under local privacy laws or otherwise from employees and other individuals to access relevant data; and
- b) Ensuring that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, z10, zSeries, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or web site are properties of their respective owners.

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

**Notice on Export Controls.** The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.



# Contents

<b>Preface.....</b>	<b>xi</b>
Intended audience . . . . .	.xi
Product version . . . . .	.xi
Syntax notation . . . . .	xii
Related documents. . . . .	xii
Getting help. . . . .	xv
Comments . . . . .	xv
 <b>1 Introduction to Hitachi Content Platform.....</b>	 <b>1</b>
About Hitachi Content Platform . . . . .	2
Object-based storage . . . . .	2
Namespaces and tenants . . . . .	3
Namespace access . . . . .	4
Namespace access protocols . . . . .	5
HCP Namespace Browser . . . . .	6
HCP metadata query API . . . . .	6
HCP Search Console . . . . .	7
HCP Data Migrator . . . . .	8
Object representation . . . . .	9
 <b>2 Tenant and namespace properties.....</b>	 <b>13</b>
Namespace quota. . . . .	14
Storage quotas. . . . .	14
Data protection level. . . . .	15
Cryptographic hash algorithm . . . . .	16
Retention mode . . . . .	16
Namespace owner . . . . .	18
Namespace tags. . . . .	19
Default retention setting . . . . .	19

Default shred setting . . . . .	20
Default index setting. . . . .	20
Default POSIX UID, GID, and permissions. . . . .	21
Retention-related properties . . . . .	22
Ownership and permission changes for objects under retention . . . . .	22
Custom metadata operations for objects under retention . . . . .	22
XML checking for custom metadata . . . . .	23
Versioning . . . . .	23
Compatibility properties . . . . .	24
Disposition. . . . .	25
Data access permission masks. . . . .	26
Minimum data access permissions . . . . .	28
Access control lists . . . . .	30
Replication. . . . .	32
Replication benefits . . . . .	32
Replication implementation . . . . .	33
Replication collision handling . . . . .	34
Object content collisions . . . . .	34
System metadata collisions . . . . .	36
Custom metadata collisions . . . . .	39
Access control list collisions . . . . .	41
Configuration collisions . . . . .	42
Retention class collisions . . . . .	44
Service plans . . . . .	45
System-level administrative access. . . . .	46
<b>3 General administrative information.....</b>	<b>47</b>
Tenant Management Console . . . . .	48
Tenant Management Console URL . . . . .	50
Logging in . . . . .	51
Using the Tenant Management Console . . . . .	53
Refreshing pages . . . . .	54
Submitting changes . . . . .	54
Viewing HCP documentation . . . . .	55
Changing your password . . . . .	55
Logging out . . . . .	56
Administrative responsibilities . . . . .	56
<b>4 Managing accounts .....</b>	<b>61</b>
About user and group accounts . . . . .	62
Administrative roles and permissions . . . . .	64
Available roles . . . . .	64

Permissions granted by roles . . . . .	65
Data access permissions . . . . .	69
User authentication. . . . .	70
Starter account . . . . .	73
Working with user accounts. . . . .	74
About the Users page . . . . .	75
Understanding the user account list . . . . .	75
Managing the user account list. . . . .	76
Creating a user account . . . . .	77
Modifying a user account and its roles . . . . .	79
Deleting a user account . . . . .	80
Working with group accounts . . . . .	81
About the Groups page . . . . .	82
Creating group accounts . . . . .	83
Modifying a group account . . . . .	85
Deleting a group account . . . . .	85
Changing the allow namespace management property for a user or group account	86
Changing the data access permissions for a user or group account . . . . .	86
Specifying permissions for any number of namespaces . . . . .	87
Changing the permissions for an individual namespace . . . . .	89
Dissociating a namespace from a user or group account . . . . .	90
Changing user account and login settings . . . . .	90
<b>5 Managing the current tenant.....</b>	<b>95</b>
About the tenant Overview page . . . . .	96
Tenant statistics . . . . .	96
Major tenant events . . . . .	97
Tenant alerts . . . . .	98
Tenant features . . . . .	98
Tenant contact information . . . . .	100
Tenant permission mask . . . . .	100
Tenant description . . . . .	100
Configuring the tenant . . . . .	101
Changing the tenant contact information . . . . .	102
Changing the tenant permission mask . . . . .	103
Changing the tenant description . . . . .	104
Enabling or disabling system-level administrative access . . . . .	104
Controlling access to the Tenant Management Console . . . . .	105
Controlling access to HCP through the management API . . . . .	106
Controlling access to the Search Console . . . . .	107
Monitoring the tenant . . . . .	108
Viewing the complete tenant event log . . . . .	109

Viewing the tenant security log . . . . .	110
Viewing the tenant compliance log . . . . .	110
Understanding log messages . . . . .	111
Managing the message list . . . . .	112
Enabling syslog logging . . . . .	113
Enabling SNMP logging . . . . .	113
Configuring email notification . . . . .	114
Enabling email notification . . . . .	115
Testing email notification . . . . .	115
Constructing the email message template . . . . .	116
Specifying email recipients . . . . .	119
Monitoring and managing replication . . . . .	121
Tenant-level view of replication . . . . .	121
Managing the namespace list . . . . .	122
Namespace-level view of replication . . . . .	123
Up-to-date-as-of time . . . . .	124
Data transmission rate . . . . .	124
Operation rate . . . . .	125
Selecting or deselecting namespaces for replication . . . . .	125
Generating chargeback reports . . . . .	127
About chargeback reports . . . . .	127
Generating a chargeback report . . . . .	128
Chargeback statistics collection . . . . .	129
Chargeback report content . . . . .	130
Sample chargeback report . . . . .	132
<b>6 Managing namespaces . . . . .</b>	<b>135</b>
About the Namespaces page . . . . .	136
Understanding the namespace list . . . . .	136
Managing the namespace list . . . . .	137
About the namespace Overview panel . . . . .	138
Namespace URL . . . . .	138
Namespace owner . . . . .	139
Objects section . . . . .	140
Usage section . . . . .	141
Major namespace events . . . . .	142
Namespace alerts . . . . .	142
Namespace features . . . . .	143
Namespace permission mask . . . . .	144
Namespace description . . . . .	144
Creating a namespace . . . . .	144
Configuring a namespace . . . . .	149
Changing the namespace name . . . . .	150

Changing the namespace permission mask . . . . .	151
Changing the namespace description . . . . .	152
Changing namespace storage quotas . . . . .	152
Changing the namespace owner . . . . .	153
Changing namespace tags. . . . .	154
Changing the default retention setting . . . . .	155
Changing the default shred setting. . . . .	157
Changing the default index setting. . . . .	158
Changing minimum data access permissions . . . . .	159
Enabling the use of ACLs. . . . .	160
Changing the option to enforce ACLs . . . . .	161
Changing retention-related settings . . . . .	161
Enabling or disabling XML checking for custom metadata . . . . .	163
Configuring object versioning. . . . .	164
Changing compatibility settings . . . . .	166
Changing disposition settings. . . . .	167
Changing replication options . . . . .	168
Changing the service plan . . . . .	169
Changing the retention mode . . . . .	170
Changing the default settings for namespace creation . . . . .	171
Setting the maximum number of namespaces per user . . . . .	173
Monitoring a namespace . . . . .	174
Viewing the complete namespace event log . . . . .	174
Viewing the namespace compliance log . . . . .	175
Working with irreparable objects . . . . .	175
Deleting a namespace. . . . .	177

## 7 [Configuring namespace access protocols.....](#) 179

Namespace access protocol configuration . . . . .	180
Protocol optimizing a namespace . . . . .	181
IP addresses for namespace access . . . . .	182
Adding and removing entries in Allow and Deny lists . . . . .	182
Valid Allow and Deny list entries . . . . .	182
Allow and Deny list handling . . . . .	183
User authentication options . . . . .	184
Configuring the HTTP, HS3, and WebDAV protocols. . . . .	185
HTTP, HS3, and WebDAV protocol configuration . . . . .	185
Considerations for the HS3 API . . . . .	187
Enabling HTTP, HS3, and WebDAV access to a namespace. . . . .	187
Configuring the CIFS protocol . . . . .	191
CIFS protocol configuration . . . . .	191
CIFS case sensitivity . . . . .	192
Enabling CIFS access to a namespace . . . . .	194
Configuring the NFS protocol. . . . .	195

NFS protocol configuration . . . . .	195
Enabling NFS access to a namespace . . . . .	195
Configuring the SMTP protocol. . . . .	196
SMTP protocol configuration . . . . .	196
Enabling SMTP access to a namespace . . . . .	197
Configuring Microsoft Exchange for email archiving through SMTP . . . . .	198
Configuring Microsoft Exchange 2003 . . . . .	199
Configuring Microsoft Exchange 2007 . . . . .	201
Configuring Microsoft Exchange 2010 . . . . .	202
<b>8 Managing search and indexing.....</b>	<b>203</b>
About search and indexing . . . . .	204
Content classes and content properties . . . . .	206
Metadata query engine indexing of custom metadata. . . . .	207
Content class and content property workflow . . . . .	208
Content property definitions . . . . .	209
Content property names . . . . .	210
Content property expressions . . . . .	212
Content property data types . . . . .	215
Formats for the integer and float data types . . . . .	216
Datetime data type formats . . . . .	219
Multivalued content properties . . . . .	221
Content properties extracted from sample XML . . . . .	221
Content property files . . . . .	223
About the Search page . . . . .	226
Managing the content class list . . . . .	226
Understanding the content property list for a content class. . . . .	227
Creating a content class . . . . .	228
Managing content properties for a content class . . . . .	228
Adding, modifying, and deleting content properties . . . . .	228
Adding content properties individually . . . . .	229
Extracting content properties from sample XML . . . . .	230
Importing content properties from a content property file. . . . .	230
Testing content properties. . . . .	231
Exporting content properties . . . . .	231
Changing the namespaces associated with a content class . . . . .	232
Reindexing namespaces associated with a content class. . . . .	233
Renaming a content class . . . . .	235
Deleting a content class . . . . .	235
Managing search and indexing for an individual namespace . . . . .	236
Setting search and indexing options . . . . .	238



Reindexing an individual namespace . . . . .	239
<b>9 Working with retention classes . . . . .</b>	<b>241</b>
About retention classes . . . . .	242
Understanding the retention class list . . . . .	243
Creating a retention class . . . . .	244
Modifying a retention class . . . . .	245
Deleting a retention class . . . . .	245
<b>10 Using privileged delete . . . . .</b>	<b>247</b>
About privileged delete . . . . .	248
Object specification . . . . .	248
Performing a privileged delete . . . . .	249
<b>11 Downloading HCP Data Migrator . . . . .</b>	<b>251</b>
HCP-DM system requirements . . . . .	252
Downloading the HCP-DM installation file . . . . .	252
<b>A Tenant Management Console alerts . . . . .</b>	<b>253</b>
Tenant Overview page alerts . . . . .	254
Namespaces page alerts . . . . .	255
Namespace Overview panel alerts . . . . .	256
Search page alert . . . . .	257
Users page alert . . . . .	258
<b>B Tenant log messages . . . . .</b>	<b>259</b>
<b>C Browser configuration for single sign-on with Active Directory . . . . .</b>	<b>269</b>
Configuring Windows Internet Explorer for single sign-on . . . . .	270
Configuring Mozilla Firefox for single sign-on . . . . .	271
<b>Glossary . . . . .</b>	<b>273</b>
<b>Index . . . . .</b>	<b>291</b>





# Preface

This book explains how to use **Hitachi Content Platform (HCP)** to monitor and manage tenants and namespaces in an HCP system. It presents the concepts and instructions you need to set up user accounts, create namespaces, configure the namespace access protocols, manage the search feature, and download the HCP Data Migrator installation files. It also covers activities you can perform to keep namespaces in compliance with local regulations.

This book does not address the default tenant and namespace. For information on managing them, see *Managing the Default Tenant and Namespace*.



---

**Note:** Throughout this book, the word *Unix* is used to represent all UNIX<sup>®</sup>-like operating systems (such as UNIX itself or Linux<sup>®</sup>).

---

## Intended audience

This book is intended for tenant administrators who configure, monitor, and manage HCP namespaces. It assumes you are familiar with your client operating system and the web browser you use to run the HCP Tenant Management Console.

## Product version

This book applies to release 7.1 of HCP.

## Syntax notation

The table below describes the conventions used for the syntax of commands, expressions, URLs, and object names in this book.

Notation	Meaning	Example
<b>boldface</b>	Type exactly as it appears in the syntax (if the context is case insensitive, you can vary the case of the letters you type)	This book shows: <b>https://tenant-url-name.hcp-name.domain-name:8000</b> You enter: https://finance.hcp-ma.example.com:8000
<i>italics</i>	Replace with a value of the indicated type	

## Related documents

The following documents contain additional information about Hitachi Content Platform:

- *Administering HCP* — This book explains how to use an HCP system to monitor and manage a digital object repository. It discusses the capabilities of the system, as well as its hardware and software components. The book presents both the concepts and instructions you need to configure the system, including creating the tenants that administer access to the repository. It also covers the processes that maintain the integrity and security of the repository contents.
- *Managing the Default Tenant and Namespace* — This book contains complete information for managing the default tenant and namespace in an HCP system. It provides instructions for changing tenant and namespace settings, configuring the protocols that allow access to the namespace, managing search and indexing, and downloading installation files for HCP Data Migrator. It also explains how to work with retention classes and the privileged delete functionality.
- *Replicating Tenants and Namespaces* — This book covers all aspects of tenant and namespace replication. Replication is the process of keeping selected tenants and namespaces in two or more HCP systems in sync with each other to ensure data availability and enable disaster recovery. The book describes how replication works, contains instructions for working with replication links, and explains how to manage and monitor the replication process.

- *HCP Management API Reference* — This book contains the information you need to use the HCP management API. This RESTful HTTP API enables you to create and manage tenants and namespaces programmatically. The book explains how to use the API to access an HCP system, specify resources, and update and retrieve resource properties.
- *Using a Namespace* — This book describes the properties of objects in HCP namespaces. It provides instructions for accessing namespaces by using the HTTP, WebDAV, CIFS, and NFS protocols for the purpose of storing, retrieving, and deleting objects, as well as changing object metadata such as retention and shred settings. It also explains how to manage namespace content and view namespace information in the Namespace Browser.
- *Using the HCP HS3 API* — This book contains the information you need to use the HCP HS3 API. This S3™-compatible, RESTful, HTTP-based API enables you to work with buckets and objects in HCP. The book introduces the HCP concepts you need to understand in order to use HS3 effectively and contains instructions and examples for each of the bucket and object operations you can perform with HS3.
- *Using the HCP OpenStack Swift API* — This book contains the information you need to use the HCP OpenStack Swift API. This S3™-compatible, RESTful, HTTP-based API enables you to work with containers and objects in HCP. The book introduces the HCP concepts you need to understand in order to use HSwift effectively and contains instructions and examples for each of the container and object operations you can perform with HSwift.
- *Using the Default Namespace* — This book describes the file system HCP uses to present the contents of the default namespace. It provides instructions for accessing the namespace by using the HCP-supported protocols for the purpose of storing, retrieving, and deleting objects, as well as changing object metadata such as retention and shred settings.
- *HCP Metadata Query API Reference* — This book describes the HCP metadata query API. This RESTful HTTP API enables you to query namespaces for objects that satisfy criteria you specify. The book explains how to construct and perform queries and describes query results. It also contains several examples, which you can use as models for your own queries.

- *Searching Namespaces* — This book describes the HCP Search Console (also called the Metadata Query Engine Console). It explains how to use the Console to search namespaces for objects that satisfy criteria you specify. It also explains how to manage and manipulate queries and search results. The book contains many examples, which you can use as models for your own searches.
- *Using HCP Data Migrator* — This book contains the information you need to install and use HCP Data Migrator (HCP-DM), a utility that works with HCP. This utility enables you to copy data between local file systems, namespaces in HCP, and earlier HCAP archives. It also supports bulk delete operations and bulk operations to change object metadata. Additionally, it supports associating custom metadata and ACLs with individual objects. The book describes both the interactive window-based interface and the set of command-line tools included in HCP-DM.
- *Installing an HCP System* — This book provides the information you need to install the software for a new HCP system. It explains what you need to know to successfully configure the system and contains step-by-step instructions for the installation procedure.
- *Deploying an HCP-VM System* — This book contains all the information you need to install and configure an HCP-VM system. The book also includes requirements and guidelines for configuring the VMWare® environment in which the system is installed.
- *Third-Party Licenses and Copyrights* — This book contains copyright and license information for third-party software distributed with or embedded in HCP.
- *HCP-DM Third-Party Licenses and Copyrights* — This book contains copyright and license information for third-party software distributed with or embedded in HCP Data Migrator.
- *Installing an HCP SAIN System — Final On-site Setup* — This book contains instructions for deploying an assembled and configured single-rack HCP SAIN system at a customer site. It explains how to make the necessary physical connections and reconfigure the system

for the customer computing environment. It also contains instructions for configuring Hi-Track<sup>®</sup> Monitor to monitor the nodes in an HCP system.

- *Installing an HCP RAIN System — Final On-site Setup* — This book contains instructions for deploying an assembled and configured HCP RAIN system at a customer site. It explains how to make the necessary physical connections and reconfigure the system for the customer computing environment. The book also provides instructions for assembling the components of an HCP RAIN system that was ordered without a rack and for configuring Hi-Track Monitor to monitor the nodes in an HCP system.

## Getting help

The Hitachi Data Systems<sup>®</sup> customer support staff is available 24 hours a day, seven days a week. If you need technical support, call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526



---

**Note:** If you purchased HCP from a third party, please contact your authorized service provider.

---

## Comments

Please send us your comments on this document:

[HCPDocumentationFeedback@hds.com](mailto:HCPDocumentationFeedback@hds.com)

Include the document title, number, and revision, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems.

**Thank you!**





# Introduction to Hitachi Content Platform

**Hitachi Content Platform (HCP)** is a distributed storage system designed to support large, growing repositories of fixed-content data.

HCP stores objects that include both data and metadata that describes that data. HCP represents these objects either as URLs or as files in a standard file system.

An HCP repository is partitioned into namespaces. Each namespace consists of a distinct logical grouping of objects with its own directory structure. Namespaces are owned and managed by tenants.

HCP provides access to objects through a variety of industry-standard protocols, as well as through various HCP-specific interfaces.

This chapter contains an overview of Hitachi Content Platform.

## About Hitachi Content Platform

Hitachi Content Platform is the distributed, fixed-content, data storage system from Hitachi Data Systems®. HCP provides a cost-effective, scalable, easy-to-use repository that can accommodate all types of data, from simple text files to medical images to multigigabyte database images.

A **fixed-content storage system** is one in which the data cannot be modified. HCP uses write-once, read-many (WORM) storage technology and a variety of policies and internal processes to ensure the integrity of the stored data and the efficient use of storage capacity. HCP also provides easy access to the repository for adding, retrieving, and deleting or shredding data.

## Object-based storage

HCP stores **objects** in a repository. Each object permanently associates data HCP receives (for example, a document, an image, or a movie) with information about that data, called **metadata**.

An object encapsulates:

- **Fixed-content data** — An exact digital reproduction of data as it existed before it was stored in HCP. Once it's in the repository, this fixed-content data cannot be modified.
- **System metadata** — System-managed properties that describe the fixed-content data (for example, its size and creation date). System metadata includes policies, such as retention and data protection level, that influence how transactions and internal processes affect the object.
- **Custom metadata** — Optional metadata that a user or application provides to further describe the object. Custom metadata is specified as one or more **annotations**, where each annotation is a discrete unit of information about the object. Annotations are typically specified in XML format.

You can use custom metadata to create self-describing objects. Users and applications can use this metadata to understand and repurpose object content.

- **Access control list (ACL)** — Optional metadata consisting of a set of grants of permissions to perform various operations on the object. Permissions can be granted to individual users or to groups of users.

ACLs are provided by users or applications and are specified in either XML or JSON format.

HCP can store multiple versions of an object, thus providing a history of how the data has changed over time. Each version is a separate object, with its own system metadata and, optionally, its own custom metadata and ACL.

HCP supports appendable objects. An **appendable object** is one to which data can be added after it has been successfully stored. Appending data to an object does not modify the original fixed-content data, nor does it create a new version of the object. Once the new data is added to the object, that data also cannot be modified.

## Namespaces and tenants

An HCP repository is partitioned into namespaces. A **namespace** is a logical grouping of objects such that the objects in one namespace are not visible in any other namespace.

Namespaces provide a mechanism for separating the data stored for different applications, business units, or customers. For example, you could have one namespace for accounts receivable and another for accounts payable.

Namespaces also enable operations to work against selected subsets of objects. For example, you could perform a query that targets the accounts receivable and accounts payable namespaces but not the employees namespace.

Namespaces are owned and managed by administrative entities called **tenants**. A tenant typically corresponds to an organization, such as a company or a division or department within a company.

In addition to being owned by a tenant, each HCP namespace can have an owner that corresponds to an individual HCP user. The owner of a namespace automatically has permission to perform certain operations on that namespace.

Each tenant can own multiple namespaces. An HCP system can have a maximum of 1,000 locally defined tenants and 10,000 locally defined namespaces. The system configuration can limit the number of namespaces an individual tenant can own.



---

**Note:** Replication can cause an HCP system to have more than 1,000 tenants and 10,000 namespaces. For information on replication, see [“Replication”](#) on page 32.

---

An HCP system has both system-level and tenant-level administrators:

- **System-level administrators** are concerned with monitoring the HCP system hardware and software, monitoring overall repository usage, configuring features that apply across the HCP system, and managing system-level users.
- **Tenant-level administrators** are concerned with monitoring namespace usage at the tenant and namespace level, configuring individual namespaces, managing tenant-level users, and controlling access to namespaces.

System-level administrators create tenants. Tenant-level administrators create namespaces. System-level administrators can limit the number of namespaces an individual tenant can own.

## Namespace access

HCP supports access to namespace content through:

- Several namespace access protocols
- The HCP Namespace Browser
- The HCP metadata query API
- The HCP Search Console
- HCP Data Migrator

## Namespace access protocols

HCP supports access to namespace content through several industry-standard protocols:

- A RESTful HTTP API (simply referred to as HTTP in the HCP documentation).
- HS3, which is a RESTful, HTTP-based API that's compatible with Amazon<sup>®</sup> S3. With HS3, namespaces are called **buckets**.
- HSwift, which is a RESTful, HTTP-based API that's compatible with OpenStack Swift. With HSwift, namespaces are called **containers**.
- WebDAV.
- CIFS.
- NFS.

These protocols support various operations: storing data, creating directories, viewing object data and metadata, viewing directories, modifying certain metadata, and deleting objects. You can use these protocols to access data with a web browser, third-party applications, Windows<sup>®</sup> Explorer, and other native Windows and Unix tools.

HCP allows special-purpose access to namespaces through the SMTP protocol. This protocol is used only for storing email.

The namespace access protocols are configured separately for each namespace and are enabled or disabled independently of each other.

The HTTP, HS3, HSwift, and CIFS protocols can be configured to require authentication. To use a protocol that requires authentication, users and applications must present valid credentials for access to the namespace.

If the HTTP, HS3, HSwift, or CIFS protocol is enabled but is not configured to require authentication or if the WebDAV or NFS protocol is enabled, users and applications can access the namespace anonymously. You can create a secure namespace by enabling only protocols that require authentication.

For information on enabling and configuring the namespace access protocols, see [Chapter 7, “Configuring namespace access protocols,”](#) on page 179. For information on using the namespace access protocols other than HS3, see *Using a Namespace*. For information on using HS3, see *Using the HCP HS3 API*.

## HCP Namespace Browser

The HCP Namespace Browser lets you manage content in and view information about namespaces. With the Namespace Browser, you can:

- List, view, and retrieve objects, including old versions of objects
- View custom metadata and ACLs for objects, including old versions of objects
- Store and delete objects
- Create empty directories
- Display namespace information, including:
  - The namespaces that you own or can access
  - Retention classes available for a given namespace
  - Permissions for namespace access
  - Namespace statistics such as the number of objects in a given namespace or the total capacity of the namespace

For information on using the Namespace Browser, see *Using a Namespace*.

## HCP metadata query API

The **HCP metadata query API** lets you search HCP for objects that meet specified criteria. The API supports two types of queries:

- **Object-based queries** search for objects based on object metadata. This includes both system metadata and the content of custom metadata and ACLs. The query criteria can also include the object location (that is, the namespace and/or directory that contains the object). These queries use a robust query language that lets you combine search criteria in multiple ways.

Object-based queries search only for objects that currently exist in the repository. For objects with multiple versions, object-based queries return only the current version.

- **Operation-based queries** search not only for objects currently in the repository but also for information about objects that have been deleted by a user or application, deleted through disposition, purged, or pruned. For namespaces that support versioning, operation-based queries can return both current and old versions of objects.

Criteria for operation-based queries can include object status (for example, created or deleted), change time, index setting, and location.

The metadata query API returns object metadata only, not object data. The metadata is returned either in XML format, with each object represented by a separate element, or in JSON format, with each object represented by a separate name/value pair. For queries that return large numbers of objects, you can use paged requests.

For information on using the metadata query API, see *HCP Metadata Query API Reference*.

## HCP Search Console

The **HCP Search Console** is an easy-to-use web application that lets you search for and manage objects based on specified criteria. For example, you can search for objects that were stored before a certain date or that are larger than a specified size. You can then delete the objects listed in the search results or prevent those objects from being deleted. Similar to the metadata query API, the Search Console returns only object metadata, not object data.

By offering a structured environment for performing searches, the Search Console facilitates e-discovery, namespace analysis, and other activities that require the user to examine the contents of namespaces. From the Search Console, you can:

- Open objects
- Perform bulk operations on objects
- Export search results in standard file formats for use as input to other applications
- Publish feeds to make search results available to web users

The Search Console works with either of these two search facilities:

- The **HCP metadata query engine** — This facility is integrated with HCP and works internally to perform searches and return results to the Search Console. The metadata query engine is also used by the metadata query API.



---

**Note:** When working with the metadata query engine, the Search Console is called the **Metadata Query Engine Console**.

---

- The **Hitachi Data Discovery Suite (DDS) search facility** — This facility interacts with HDDS, which performs searches and returns results to the HCP Search Console. HDDS is a separate product from HCP.

The Search Console can use only one search facility at any given time. The search facility is selected at the HCP system level. If no facility is selected, the HCP system does not support use of the Search Console to search namespaces.

Each search facility maintains its own index of objects in each search-enabled namespace and uses this index for fast retrieval of search results. The search facilities automatically update their indexes to account for new and deleted objects and changes to object metadata.

To learn which search facility, if any, is selected for the HCP Search Console, contact your HCP system administrator. For more information on the search indexes, see [“About search and indexing”](#) on page 204. For information on using the Search Console, see *Searching Namespaces*.

## HCP Data Migrator

**HCP Data Migrator (HCP-DM)** is a high-performance, multithreaded, client-side utility for viewing, copying, and deleting data. With HCP-DM, you can:

- Copy objects, files, and directories between the local file system, HCP namespaces, default namespaces, and earlier HCAP archives
- Delete individual objects, files, and directories and perform bulk delete operations
- View the content of current and old versions of objects and the content of files



- Purge all versions of an object
- Rename files and directories on the local file system
- View object, file, and directory properties
- Change system metadata for multiple objects in a single operation
- Add, replace, or delete custom metadata for objects
- Add, replace, or delete ACLs for objects
- Create empty directories

HCP-DM has both a graphical user interface (GUI) and a command-line interface (CLI).

For information on downloading HCP-DM, see [Chapter 11, “Downloading HCP Data Migrator.”](#) on page 251. For information on installing and using HCP-DM, see *Using HCP Data Migrator*.

## Object representation

HCP represents objects differently based on the namespace access protocol the client is using.

### Object representation with HTTP

With HTTP, HCP represents each object as a URL. The root of the object path in the URL is always `rest`.

Here’s an example of the URL for an object named `wind.jpg` in the `images` directory in a namespace named `climate` in a tenant named `geo` in an HCP system named `hcp.example.com`:

```
http://climate.geo.hcp.example.com/rest/images/wind.jpg
```

Users and applications represent system metadata and identify custom metadata by using query parameters appended to the URLs. HCP returns system metadata in HTTP response headers and returns custom metadata in the format in which it was originally specified.

For more information on object representation with HTTP, see *Using a Namespace*.

### **Object representation with the HS3 API**

With the HS3 API, HCP represents each object as a URL. The exact format of this URL depends on how the application used to access the object handles user authentication.

HS3 does not have the concept of directories. Slashes in object names are simply part of the name and are not directory separators. Thus, objects in HS3 do not have paths.

Here's an example of one of the possible URLs for an object named `images/wind.jpg` in a namespace named `climate` in a tenant named `geo` in an HCP system named `hcp.example.com`:

```
http://climate.geo.hcp.example.com/hs3/images/wind.jpg
```

Users and applications represent system and custom metadata by using HTTP request headers. HCP returns system and custom metadata in HTTP response headers.

For more information on object representation with the HS3 API, see *Using the HCP HS3 API*.

### **Object representation with the HSwift API**

With the HSwift API, HCP represents each object as a URL. The exact format of this URL depends on how the application used to access the object handles user authentication.

HSwift does not have the concept of directories. Slashes in object names are simply part of the name and are not directory separators. Thus, objects in HSwift do not have paths.

Here's an example of one of the possible URLs for an object named `images/fire.jpg` in a namespace named `climate` in a tenant named `geo` in an HCP system named `hcp.example.com`:

```
http://api.climate.geo.hcp.example.com/swift/v1/geo/climate/images/fire.jpg
```

Users and applications represent system and custom metadata by using HTTP request headers. HCP returns system and custom metadata in HTTP response headers.

For more information on object representation with the HSwift API, see *Using the HCP OpenStack HSwift API*.

**Object representation with other namespace access protocols**

For namespace access protocols other than HTTP and HS3, HCP includes a standard POSIX file system called HCP-FS that represents each object as a set of files. One of these files has the same name as the object. This file contains the fixed-content data. When downloaded or opened, this file has the same content as the originally stored item.

The other files that HCP-FS presents contain object metadata. These files, most of which are plain text, are called **metafiles**.

All files containing fixed-content data are in a directory hierarchy headed by `data`. All metafiles are in a directory hierarchy headed by `metadata`.

With this view of objects as conventional files and directories, HCP supports routine file-level calls and enables users and applications to find fixed-content data in familiar ways.

For more information on object representation with protocols other than HTTP and HS3, see *Using a Namespace*.



# Tenant and namespace properties

Tenants and namespaces have certain properties that affect how they operate. Some of these properties are set when the tenant or namespace is created. Others are set after creation. Some can be modified after they are initially set; others cannot.

This chapter addresses these properties of tenants and namespaces:

- Namespace quota
- Storage quotas
- Data protection level
- Cryptographic hash algorithm
- Retention mode
- Namespace owner
- Namespace tags
- Default retention, shred, and index settings
- Whether POSIX ownership and permission changes are allowed for objects under retention
- Which custom metadata operations are allowed for objects under retention
- XML checking for custom metadata
- Versioning

- Compatibility
- Disposition
- Data access permission masks
- Minimum data access permissions
- Access control lists
- Replication
- Service plans
- System-level administrative access

For information on the search and indexing properties of tenants and namespaces, see [Chapter 8, “Managing search and indexing.”](#) on page 203.



---

**Note:** In this chapter, in the context of namespace access, the term *users* means both people and applications.

---

## Namespace quota

The **namespace quota** for a tenant is the number of namespaces HCP reserves for the tenant out of the total number of namespaces the system can have. At any given time, the tenant can own only as many namespaces as specified by this quota.

The namespace quota is set when the tenant is created. HCP system-level administrators can change this quota at any time. However, the quota cannot be set lower than the number of namespaces the tenant currently owns.

## Storage quotas

Both tenants and namespaces have hard and soft storage quotas:

- A **hard quota** is an absolute number of bytes. For a tenant, it is the total amount of storage available to that tenant for allocation to its namespaces. For a namespace, it is the total amount of space available for storing objects in that namespace, including object data, metadata

(except ACLs), and the redundant data required to satisfy the namespace DPL. For information on DPL, see [“Data protection level”](#) on page 15.



**Note:** HCP checks the amount of data stored in a namespace against the namespace hard quota hourly. If large amounts of data are added rapidly to a namespace, the namespace can store substantially more data than its hard quota allows.

Each namespace managed by a tenant can exceed its hard quota in this way. As a result, the total amount of storage used by all the namespaces owned by the tenant can exceed the hard quota for the tenant.

- A **soft quota** is the percentage point at which HCP notifies the tenant that allocated storage space is being used up. For a tenant, the soft quota measures the space used in all the namespaces the tenant owns relative to the hard quota for that tenant. For a namespace, the soft quota measures the space used in just that namespace relative to the hard quota for that namespace.

The storage quotas for a tenant are set when the tenant is created. HCP system-level administrators can change these quotas at any time. However, the hard quota for a tenant cannot be set lower than the amount of space the tenant has currently allocated to its namespaces.

The storage quotas for a namespace are set when the namespace is created. You can change these quotas at any time. However, the hard quota for a namespace cannot be set lower than the amount of space currently used in the namespace. And, the total of the hard quotas for all the namespaces owned by a tenant cannot exceed the hard quota for that tenant.

For information on changing the hard or soft quota for a namespace, see [“Changing namespace storage quotas”](#) on page 152.

## Data protection level

Each namespace has a **data protection level (DPL)** that specifies how many copies of each object HCP must maintain. HCP stores each copy of an object in a different location. All but one of these copies can become unavailable (for example, due to a hardware outage) without affecting access to the object.

The DPL for a namespace can be one (if allowed by the HCP system configuration), two, three, four, or dynamic. The highest allowed DPL is also determined by the HCP system configuration.

When the DPL is set to dynamic, the namespace uses the current HCP system-level DPL setting. Typically, this is the optimal DPL for the system configuration. If the system-level DPL setting changes, HCP adjusts the number of copies of objects in the namespace to match the new setting.

The DPL affects the amount of storage used when data is added to the namespace. With a DPL of one, HCP stores only one copy of the object. With a DPL of two, HCP stores two copies, thereby using twice as much storage.

The DPL for a namespace is set when the namespace service plan is created. You can change this setting at any time.

## Cryptographic hash algorithm

At object creation, HCP uses a cryptographic hash algorithm to calculate a hash value for the object from the object data. HCP then uses this hash value to ensure the integrity of the object over time.

HCP supports these cryptographic hash algorithms:

- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- RIPEMD-160

The cryptographic hash algorithm HCP uses for a namespace is set when the namespace is created. Once set, it cannot be changed.

## Retention mode

Each object has a **retention setting** that specifies how long the object must remain in the namespace before it can be deleted; this duration is called the **retention period**. While an object cannot be deleted due to its retention setting, it is said to be **under retention**.



**Retention mode** is a property of a namespace that affects which operations are allowed on objects under retention. A namespace can be in either of two retention modes:

- In **compliance mode**, objects that are under retention cannot be deleted through any mechanism. Additionally, the duration of a retention class cannot be shortened, and retention classes cannot be deleted.
- In **enterprise mode**, you can use the Tenant Management Console to delete objects under retention if you have the compliance role. This is called **privileged delete**.

Also in enterprise mode, you can shorten the duration of a retention class, and you can delete retention classes.



**Note:** Users can perform privileged deletes in a namespace that's in enterprise mode. To do this, however, they need the privileged data access permission.

---

The retention mode for a namespace is set when the namespace is created. You can change the retention mode of a namespace from enterprise to compliance mode but cannot do the reverse.

You can create namespaces in compliance mode only if allowed to do so by the tenant configuration. HCP system-level administrators can change this configuration from not allowing the creation of namespaces in compliance mode to allowing it. However, they cannot do the reverse.

For information on:

- Changing the retention mode of a namespace, see [“Changing the retention mode”](#) on page 170
- Retention settings, see [“Changing the default retention setting”](#) on page 155
- Retention classes, see [Chapter 9, “Working with retention classes.”](#) on page 241
- Privileged delete, see [Chapter 10, “Using privileged delete.”](#) on page 247
- Roles, see [“Administrative roles and permissions”](#) on page 64
- Data access permissions, see [“Data access permissions”](#) on page 69

## Namespace owner

A namespace can optionally have an owner that corresponds to an HCP or Active Directory® (AD) user. Assuming that the user has the allow namespace management property, the owner of a namespace can use the HS3 and HCP management APIs to:

- View and change the versioning status of the namespace
- Delete the namespace
- See the namespace in a namespace listing

You can also use the Tenant Management Console and HCP management API to perform these activities if you have the administrator role, even if you're not the namespace owner.

You can specify the owner of a namespace when you create the namespace or at any time thereafter. You can also change namespace owners at any time.

When the HS3 API is used to create a namespace, the namespace creator automatically becomes the namespace owner.

When a user with an HCP user account becomes the owner of a namespace, that user account automatically gets the browse, read, write, read ACL, and write ACL data access permissions for that namespace. If HS3 was used to create the namespace, the owner user account also automatically gets the delete permission for the namespace.

You can limit the number of namespaces that can be owned by a single user. You can change this limit at any time.

For information on:

- The allow namespace management property, see ["About user and group accounts"](#) on page 62
- Using the HS3 API, see *Using the HCP HS3 API*
- Using the HCP management API, see *HCP Management API Reference*
- The Tenant Management Console, see ["Tenant Management Console"](#) on page 48

- Changing namespace owners, see [“Changing the namespace owner”](#) on page 153
- Changing the limit on namespace ownership, see [“Setting the maximum number of namespaces per user”](#) on page 173

## Namespace tags

A tag is an arbitrary text string associated with a namespace. You can associate up to ten tags with any given namespace, and you can use the same tags for multiple namespaces.

You can use tags to group namespaces and filter namespace lists. For example, if you’ve created multiple namespaces for a company named ABC Corporation, you could associate the tag ABC with each of those namespaces. Then you could filter a list of namespaces to display only the namespaces with that tag.

You can associate tags with a namespace when you create the namespace or at any time thereafter. You can also remove tags from a namespace at any time.

For information on associating tags with namespaces, see [“Changing namespace tags”](#) on page 154.

## Default retention setting

Each namespace has a default retention setting. This is the setting applied to an object when it is stored in the namespace unless the retention setting is explicitly specified in the request to store the object. After an object is stored, users can change its retention setting (subject to the rules for changing retention settings).

When you create a namespace, its default retention setting is **Deletion Allowed**. Objects with this retention setting can be deleted at any time except when they’re on hold.

You can change the default retention setting for a namespace at any time. Changing this setting does not affect existing objects in the namespace.

For information on changing the default retention setting, see [“Changing the default retention setting”](#) on page 155. For more information on retention settings in general, see *Using a Namespace*.

## Default shred setting

**Shredding**, also called **secure deletion**, is the process of overwriting the places where all the copies of an object were stored in such a way that none of the object data or metadata, including custom metadata, can be reconstructed. Each object has a shred setting that determines whether it is shredded when it's deleted from the namespace.

Each namespace has a default shred setting. This is the setting applied to an object when it is stored in the namespace unless the shred setting is explicitly specified in the request to store the object. After an object is stored, users can change its shred setting from don't shred to shred but not from shred to don't shred.

When you create a namespace, its default shred setting is not to shred. You can change this setting at any time. Changing this setting does not affect existing objects in the namespace.

For information on changing the default shred setting, see ["Changing the default shred setting"](#) on page 157.

## Default index setting

Each object in the repository has an index setting that is either **true** or **false**. This setting is present even if the namespace containing the object is not search-enabled or indexed.

The metadata query engine uses the index setting for an object to determine whether to index custom metadata for that object. The HCP search facility uses the index setting to determine whether to index the object at all. Metadata query API requests can use the index setting as a search criterion. Additionally, third-party applications can use this setting for their own purposes.



---

**Note:** If custom metadata indexing is disabled, the metadata query engine does not index custom metadata regardless of the index settings for individual objects. For more information on custom metadata indexing, see ["Metadata query engine indexing of custom metadata"](#) on page 207.

---

Each namespace has a default index setting. This is the setting applied to an object when it is stored in that namespace unless the index setting is explicitly specified in the request to store the object. After an object is stored, users can change its index setting.

When you create a namespace, its default index setting is to index. You can change this setting at any time. Changing this setting does not affect existing objects in the namespace.

For information on changing the default index setting, see [“Changing the default index setting”](#) on page 158.

## Default POSIX UID, GID, and permissions

To support the NFS protocol, HCP supports certain POSIX metadata for objects. This metadata includes the POSIX user ID (UID) of the object owner, the POSIX group ID (GID) of the owning group, and the POSIX permissions.




---

### Notes:

- POSIX object ownership is different from object ownership in HCP. The owner UID is not related to either HCP user accounts or Active Directory user accounts.
  - POSIX permissions are different from HCP data access permissions and access control lists. They affect the operations that clients can perform only through the CIFS and NFS protocols.
- 

POSIX UIDs and GIDs are visible through the HTTP, WebDAV, CIFS, and NFS protocols. POSIX permissions are visible through the WebDAV and NFS protocols. They map to CIFS permissions, which are visible through the CIFS protocol.

For objects stored through NFS, the POSIX UID and GID are determined by the current NFS user. Objects stored through other protocols do not have an explicit UID or GID. Instead, when you use NFS to view these properties for such an object, you see the default UID and GID currently specified in the NFS protocol configuration for the namespace that contains the object.

When you create a namespace, the default UID and GID in the NFS protocol configuration are both set to 0 (zero). You can change these settings at any time.

POSIX permissions for objects, directories, and symbolic links stored through NFS are determined by the client. POSIX permissions for objects stored through other protocols are always 555. POSIX permissions for directories and symbolic links stored through other protocols are always 777.

For information on changing the default UID and GID in the NFS protocol configuration, see [“Configuring the NFS protocol”](#) on page 195.

## Retention-related properties

Namespaces have two properties that affect objects under retention:

- Whether changes to POSIX UIDs and GIDs and to object owners are allowed
- Which custom metadata operations are allowed

## Ownership and permission changes for objects under retention

POSIX UIDs, GIDs, and permissions are changeable only through the CIFS and NFS protocols. Changes to object owners are possible only through the HTTP protocol.

Whether users can change these properties for objects under retention is a property of a namespace. When the namespace is created, these changes are not allowed. You can change this setting at any time.

For information on changing the setting for ownership and permission changes for objects under retention, see [“Changing retention-related settings”](#) on page 161. For more information on object ownership and permissions in general, see *Using a Namespace*.

## Custom metadata operations for objects under retention

Custom metadata is user-supplied information that describes an object in a namespace. For objects that are not under retention, users can add, replace, and delete custom metadata annotations as needed. For objects that are under retention, the operations allowed for custom metadata annotations are determined by a namespace-level setting.

You can configure a namespace to:

- Allow annotations to be added, replaced, and deleted for objects under retention
- Allow annotations to be added for objects under retention but not replaced or deleted
- Disallow all annotations operations for objects under retention

When you create a namespace, only the addition of annotations is allowed for objects under retention. You can change this setting at any time.

For information on changing custom metadata handling for a namespace, see [“Changing retention-related settings”](#) on page 161. For more information on custom metadata in general, see *Using a Namespace*.

## XML checking for custom metadata

By default, when a custom metadata annotation is added to or replaced in a namespace, HCP checks whether it contains well-formed XML. If the XML is not well-formed, HCP rejects the annotation.

For any given namespace, you can choose to allow users to provide annotations in non-XML formats (for example, as thumbnail images to accompany large objects with image content). In this case, you need to disable custom metadata XML checking for the namespace so that HCP accepts non-XML annotations.

XML checking applies only when annotations are added to or replaced in a namespace. It does not apply to annotations that already exist in the namespace.

You can enable or disable custom metadata XML checking for a namespace at any time. For instructions on doing this, see [“Enabling or disabling XML checking for custom metadata”](#) on page 163. For more information on custom metadata in general, see *Using a Namespace*.



**Note:** If the XML in an annotation for an object includes a very large number of different elements and attributes, HCP may determine that the XML is not well-formed, even if it is, and reject the annotation. If this happens, the user can try restructuring the XML so that it includes fewer different elements and attributes. Alternatively, you can temporarily disable custom metadata XML checking to allow that XML to be stored in the namespace.

## Versioning

**Versioning** is the creation of multiple versions of objects. Versioning is supported only with the HTTP and HS3 protocols. Users cannot create new versions of objects or access old versions through any other protocol.

Any given namespace can be configured to support versioning or not to support it. However, you cannot enable versioning for a namespace while the WebDAV, CIFS, NFS, or SMTP protocol or appendable objects are enabled for that namespace. Conversely, you cannot enable the WebDAV, CIFS, NFS, or SMTP protocol or appendable objects for a namespace while versioning is enabled for that namespace. You can disable versioning at any time.

When versioning is enabled for a namespace, you can set a time for version pruning. **Version pruning** is the automatic deletion of previous versions of objects that are older than a specified amount of time.

If you disable versioning after it was enabled, old versions of objects remain in the namespace and continue to be pruned according to the pruning settings. If you change the pruning settings, the new settings apply to old versions regardless of whether versioning is enabled.

You can create namespaces with versioning enabled only if allowed to do so by the tenant configuration. HCP system-level administrators can change this configuration from not allowing the creation of namespaces with versioning enabled to allowing it. However, they cannot do the reverse.

For information on changing versioning settings for a namespace, see [“Configuring object versioning”](#) on page 164.

## Compatibility properties

Namespaces have two features that support HCP compatibility with other storage products:

- Synchronization of POSIX **atime** values with retention settings. For information on the effects of this option, see *Using a Namespace*.
- Creation of appendable objects.



### Notes:

- Users can create and add data to appendable objects only through the CIFS and NFS protocols.
  - Appendable objects and versioning cannot be enabled at the same time.
-



When you create a namespace, both of these features are disabled. You can enable or disable them at any time.

For information on enabling and disabling these features, see [“Changing compatibility settings”](#) on page 166.

## Disposition

**Disposition** is the automatic deletion of objects. Disposition can be enabled for:

- Objects with expired retention periods. To be eligible for disposition, an object must have a retention setting that’s either:
  - A date in the past
  - A retention class with automatic deletion enabled that results in a calculated expiration date in the past
- Objects flagged as replication collisions.

Disposition has the benefit of automatically freeing HCP storage space for the creation of more objects. Without disposition, users need to explicitly delete qualified objects to free the occupied space.

Disposition deletes only the current version of a versioned object. It does not delete old versions.

Disposition is enabled on a per-namespace basis. When you create a namespace, this feature is disabled. You can change this setting at any time.

For information on enabling and disabling disposition, see [“Changing disposition settings”](#) on page 167. For information on retention classes, see [Chapter 9, “Working with retention classes,”](#) on page 241. For information on objects flagged as replication collisions, see [“Object content collisions”](#) on page 34.



---

**Note:** HCP system-level administrators can enable or disable disposition for the repository as a whole. While disposition is disabled for the repository, enabling it for a namespace has no effect.

---

## Data access permission masks

A **data access permission mask** determines which of these operations are allowed in a namespace:

1. **Read** — Lets users:

- View and retrieve objects, including object metadata (system metadata, custom metadata, and ACLs)
- View and retrieve previous versions of objects
- List annotations for objects
- List directory contents

2. **Write** — Lets users:

- Add objects to the namespace.
- Modify system metadata. For users to modify the hold status of objects, privileged operations must also be allowed.
- Add and replace custom metadata.
- Add, replace, and delete ACLs.
- Change object owners.

• **Delete** — Lets users delete objects and custom metadata from the namespace.

• **Purge** — Lets users delete all versions of an object with a single operation. For users to perform purge operations, delete operations must also be allowed.

3. **Privileged** — Lets users:

- Delete or purge objects that are under retention. For users to perform privileged delete operations, delete operations must also be allowed. For users to perform privileged purge operations, delete and purge operations must also be allowed.
- Hold and release objects. For users to perform hold and release operations, write operations must also be allowed.

- **Search** — Lets users use the HCP metadata query API and the HCP Search Console to query or search the namespace. For users to query or search a namespace, read operations must also be allowed.

Data access permission masks are set at the system, tenant, and namespace levels:

- The system-level mask applies across all namespaces (that is, systemwide).
- The tenant-level mask is set individually for each tenant. This mask applies only to the namespaces owned by that tenant.
- The namespace-level mask is set individually for each namespace and applies only to that namespace.

The effective permissions for a tenant are the operations allowed by both the system-level and tenant-level permission masks. That is, to be in effect for a tenant, a permission must be included in the system-level permission mask *and* in the tenant-level permission mask.

The effective permissions for a namespace are the operations that are allowed by the masks at all three levels. That is, to be in effect for a namespace, a permission must be included in the system-level permission mask, the tenant-level permission mask, *and* the namespace-level permission mask.

The table below shows an example of the effective permissions for a namespace given a set of data access permission masks.

Permission mask	Permissions					
	Read	Write	Delete	Purge	Priv. delete	Search
Systemwide permission mask	✓	✓	✓	✓		✓
Tenant permission mask	✓	✓	✓	✓	✓	
Namespace permission mask	✓	✓	✓		✓	✓
<b>Effective permission mask</b>	✓	✓	✓			

A tenant initially has all permissions in its data access permission mask. When you create a namespace, it also has all permissions in its data access permission mask.

HCP system-level administrators can change the systemwide permission mask at any time. You can change the tenant and namespace permission masks at any time.

You can make a namespace effectively read-only by removing all operations except read from its data access permission mask.

For information on setting the tenant and namespace permission masks, see [“Changing the tenant permission mask”](#) on page 103 and [“Changing the namespace permission mask”](#) on page 151.

## Minimum data access permissions

The configuration of a namespace can include minimum data access permissions for all users (that is, authenticated users and users that access the namespace anonymously) and for authenticated users only. When accessing the namespace:

- Authenticated users have all the data access permissions associated with the applicable user account or group accounts and all the minimum data access permissions for authenticated users. Additionally:
  - When using a protocol that requires authentication, authenticated users may or may not also have the minimum data access permissions for all users. This is determined by a namespace option that’s intended to support the following scenario:
    - Data can be written to the namespace only from within a secured environment and only from a limited number of client computers through a protocol such as NFS that does not support authentication. This requires write permission for all users.
    - Objects can be accessed from outside the secured environment but only through a protocol that requires authentication. This requires read permission but not write permission for authenticated users.
  - When using a protocol that does not require authentication, authenticated users also have the all minimum data access permissions for all users.

Authenticated users also have any object-specific permissions granted to them by object ACLs (see [“Access control lists”](#) below).

- Unauthenticated users (that is, users who access the namespace anonymously) have the minimum data access permissions for all users and any object-specific permissions granted to all users by object ACLs (see [“Access control lists”](#) below).

If you don't set any minimum data access permissions for all users, the only operations unauthenticated users can perform in the namespace are those for which they are granted permission by ACLs.




---

**Tip:** If you enable only namespace access protocols that don't support authentication, consider setting at least one minimum data access permission for all users.

---

For both all users and authenticated users, the set of minimum data access permissions can include only these permissions:

- **Browse** — Lets users list directory contents.
- **Read** — Lets users:
  - View and retrieve objects, including system metadata and custom metadata for objects
  - View and retrieve previous versions of objects
  - Check the existence of objects
  - List annotations for objects

For this permission to be granted, users must also have browse permission.

- **Read ACL** — Lets users view and retrieve object ACLs.
- **Write** — Lets users:
  - Add objects to the namespace
  - Modify system metadata (except retention hold)
  - Add or replace custom metadata
- **Write ACL** — Lets users add, replace, and delete object ACLs.

- **Delete** — Lets users delete objects, and custom metadata, and ACLs from the namespace.
- **Purge** — Lets users delete all versions of an object with a single operation. For this permission to be granted, users must also have delete permission.

Users with any data access permissions for a namespace can view information about that namespace.



---

**Note:** To store an object with CIFS on a Windows client, a user must have both read and write permissions.

---

When you create a namespace, the set of minimum data access permissions is empty for both all users and authenticated users. You can modify these sets at any time.

For information on:

- Changing minimum data access permissions, see [“Changing minimum data access permissions”](#) on page 159
- User and group accounts, their associated data access permissions, and user authentication, see [“About user and group accounts”](#) on page 62
- Authenticated and anonymous access to namespaces, see *Using a Namespace*

## Access control lists

A namespace can be configured to allow users to associate ACLs with objects. An ACL consists of **access control entries**. Each access control entry grants a user or group of users (the grantee) one or more data access permissions for the applicable object.

### ACL permissions

The permissions that can be included in an access control entry are:

- **Read** — Lets the grantee read and retrieve the object, including the system metadata and any custom metadata for the object, and list annotations for the object.

To read or retrieve the object through CIFS or NFS, the grantee must also have browse permission.

- **Read ACL**— Lets the grantee read and retrieve the object ACL.
- **Write** — Lets the grantee modify system metadata and add and replace custom metadata for the object.
- **Write ACL** — Lets the grantee add, replace, or delete the object ACL.
- **Delete** — Lets the grantee delete or purge the object and delete the object ACL.

For information on working with ACLs, see *Using a Namespace*.

### Use of ACLs

When you create a namespace, the use of ACLs is disabled. You can enable this feature for the namespace at any time. However, once this feature is enabled, you cannot disable it.

Users can add and replace ACLs only with the HTTP protocol. Therefore, if you enable the use of ACLs for a namespace, you should also enable that protocol.

For information on enabling the user of ACLS, see [“Enabling the use of ACLs”](#) on page 160.

### Enforcing ACLs

While the use of ACLs is enabled for a namespace, you can specify whether HCP should enforce ACLs in that namespace. While HCP is enforcing ACLs, the operations that a given user can perform on a given object are those permitted by any of:

- The data access permissions associated with the applicable user account or group accounts
- The applicable minimum data access permissions specified in the namespace configuration
- The object ACL

When not enforcing ACLs, HCP allows only the operations permitted by the first two items above.

You can change the specification of whether HCP should enforce ACLs at any time while the use of ACLs is enabled.

### More information

For more information on:

- Specifying whether HCP enforces ACLs, see [“Changing the option to enforce ACLs”](#) on page 161
- User and group accounts and their associated data access permissions, see [“About user and group accounts”](#) on page 62
- Minimum data access permissions, see [“Minimum data access permissions”](#) on page 28

## Replication

**Replication** is the process of keeping selected tenants and namespaces in two or more HCP systems in sync with each other. Basically, this entails copying object creations, deletions, and metadata changes between systems. HCP also replicates tenant and namespace configuration, user and group accounts, retention classes, content classes, all compliance log messages, and most other tenant log messages.

A **replication topology** is a configuration of HCP systems that are related to each other through replication. Typically, the systems in a replication topology are in separate geographic locations and are connected by a high-speed wide area network.

Clients can read from namespaces on all systems to which those namespaces are replicated. The replication configuration set at the system level determines on which systems clients can write to namespaces.



**Note:** Not all HCP systems support replication.

---

## Replication benefits

Replication has several purposes:

- If one system in a replication topology becomes unavailable (for example, due to network issues), another system in the topology can provide continued data availability.
- If one system in a replication topology suffers irreparable damage, another system in the topology can serve as a source for disaster recovery.



- If multiple HCP systems are widely separated geographically, each system may be able to provide faster data access for some applications than the other systems can, depending on where the applications are running.
- If an enterprise has several satellite offices, an HCP system at a central facility can consolidate data from the HCP systems at those outlying locations.
- If an object cannot be read from one system in a replication topology (for example, because a server is unavailable), HCP can try to read it from another system in the topology. HCP tries to do this only if:
  - The namespace that contains the object is being replicated.
  - The namespace has the read-from-remote-system feature enabled.
  - The object has already been replicated. Users can check object metadata to determine whether an object has been replicated.

For information on this feature, see [“Changing replication options”](#) on page 168.

- If a system that participates in a replication topology is unavailable, HTTP requests to that system can be automatically serviced by another system in the topology without the client needing to modify the target URL. The other system can service a request only if:
  - The namespace named in the URL is replicated to the other system
  - The namespace named in the URL is configured to accept requests redirected from other HCP systems
  - The HCP systems involved use DNS for system addressing

For information on enabling this feature, see [“Changing replication options”](#) on page 168.

## Replication implementation

Replication is implemented at the tenant and namespace level. When creating a tenant, the HCP system administrator specifies whether it is eligible to be replicated. HCP system administrators can change this setting from not allowing replication to allowing it. However, they cannot do the reverse.

If the tenant is eligible for replication, you can choose whether or not to include each namespace in the replication of the tenant. You can change this setting for a namespace at any time.

The HCP system administrator selects tenants to be replicated from among those that are eligible. If a tenant has granted system-level administrative users access to itself, the system administrator can change the namespace selections for that tenant. HCP replicates the configuration of each selected tenant and the configuration and contents of all the namespaces selected for replication with the tenant.

Depending on the replication topology, you may not be able to make any configuration changes to the tenant or any of its namespaces on one or more systems in the topology. Clients cannot make any changes to namespace content on systems on which you cannot make configuration changes.

Replication is asynchronous with other HCP activity. If allowed by the system configuration, you can monitor replication progress in the Tenant Management Console. For information on this and on selecting namespaces for inclusion in replication of a tenant, see [“Monitoring and managing replication”](#) on page 121.

## Replication collision handling

If clients can write to multiple systems in a replication topology, collisions can occur when different changes are made to the same objects on different systems. Similarly, if you can make configuration changes to the tenant and its namespaces on multiple systems in a replication topology, configuration collisions can occur.

The way HCP handles collisions that occur due to replication depends on the type of collision. However, the general rule is that more recent changes have priority over conflicting less recent changes.

## Object content collisions

An object content collision occurs when, for a namespace without versioning enabled, these events occur in the order shown:

1. An object is created with the same name in that namespace on two systems in a replication topology, but the object has different content on the two systems.
2. The object on one of the systems is replicated to the other system.

If versioning is enabled for the namespace, no collision occurs. Instead, the less recently created of the two objects becomes an old version of the more recently created object.

When an object content collision occurs, the more recently created object keeps its name and location. The other object is either moved to the `.lost+found` directory in the same namespace or renamed, depending on the namespace configuration.

When HCP moves an object to the `.lost+found` directory, the full object path becomes `.lost+found/replication/system-generated-directory/old-object-path`.

When renaming an object due to a content collision, HCP changes the object name to `object-name.collision` or `object-name.version-id.collision`, where `version-id` is the version ID of the object. HCP uses the second format only if versioning has ever been enabled for the namespace that contains the object but is not currently enabled.

If the new name is already in use, HCP changes the object name to `object-name.1.collision` or `object-name.version-id.1.collision`, as applicable. If that name is already in use, HCP successively increments the middle integer by one until a unique name is formed.

Objects that have been relocated or renamed due to content collisions are flagged as replication collisions in their system metadata. Clients can use the metadata query API to search for objects that are flagged as replication collisions.

If an object that's flagged as a replication collision changes (for example, if its retention period is extended), its collision flag is removed. If a client creates a copy of a flagged object with a new name, the collision flag is not set on the copy.

You can configure namespaces to have the disposition service automatically delete objects that are flagged as replication collisions. When selecting this option for a namespace, you specify the number of days the disposition service should wait before deleting such an object. The days are counted from the time the collision flag is set. If the collision flag is removed from an object, the object is no longer eligible for deletion by the disposition service.

For information on configuring the method HCP should use to handle object name collisions in a namespace, see [“Changing replication options”](#) on page 168. For information the metadata query API, see *HCP Metadata Query API Reference*.

## System metadata collisions

A system metadata collision occurs when these events occur in the order shown:

1. Different changes are made to the system metadata for a given object on each of two systems in a replication topology.
2. The changed system metadata on one of the systems is replicated to the other system.

For example, suppose a user on one system changes the shred setting for an object while a user on the other system changes the index setting for the same object. When the object on either system is replicated to the other system, a system metadata collision occurs.

If a collision occurs when changed system metadata for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- For changed system metadata other than the retention setting and hold status:
  - If the last change made on system A is more recent than the last change made on system B, HCP changes the system metadata on system B to match the system metadata on system A.
  - If the last change on system B is more recent than the last change on system A, HCP does not change the system metadata on system B.
- For a changed retention setting:
  - If the retention setting on system A specifies a longer retention period than does the retention setting on system B, HCP changes the retention setting on system B to match the retention setting on system A.
  - If the retention setting on system B specifies a longer retention period than does the retention setting on system A, HCP does not change the retention setting on system B.
- For a changed hold status:
  - If the object is on hold on system A but not on system B, HCP places the object on hold on system B.

- If the object is on hold on system B but not on system A, HCP leaves the object on hold on system B.

Here are some examples of how HCP handles collisions when changed system metadata for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology.

### Example 1

The object starts out on both system A and system B with these system metadata settings:

Shred: false  
Index: false

The table below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

Sequence	Event
1	On system A, a client changes the shred setting to true.
2	On system B, a client changes the index setting to true.
3	The changes on system A are replicated to system B. The resulting settings for the object on system B are:  Shred: false Index: true

### Example 2

The object starts out on both system A and system B with these system metadata settings:

Retention: Initial Unspecified  
Shred: false  
Index: false

The table below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

Sequence	Event
1	On system A, a client changes the retention setting to Deletion Prohibited.
2	On system B, a client changes the retention setting to Deletion Allowed.
3	On system B, a client changes the index setting to true.
4	On system A, a client changes the shred setting to true.

*(Continued)*

Sequence	Event
5	<p>The changes on system A are replicated to system B. The resulting settings for the object on system B are:</p> <p>Retention: Deletion Prohibited Shred: true Index: false</p>

**Example 3**

The object starts out on both system A and system B with these system metadata settings:

Retention: Initial Unspecified  
Hold: true  
Shred: false  
Index: false

The table below shows a sequence of events in which the system metadata for the object is changed and the changes are then replicated.

Sequence	Event
1	On system A, a client changes the retention setting to Deletion Allowed.
2	On system B, a client changes the retention setting to Deletion Prohibited.
3	On system B, a client changes the index setting to true.
4	On system A, a client changes the shred setting to true.
5	On system A, a client releases the object from hold.
6	<p>The changes on system A are replicated to system B. The resulting settings for the object on system B are:</p> <p>Retention: Deletion Prohibited Hold: true Shred: true Index: false</p>
7	<p>The changes on system B are replicated to system A. The resulting settings for the object on system A are:</p> <p>Retention: Deletion Prohibited Hold: true Shred: true Index: false</p>

## Custom metadata collisions

A custom metadata collision occurs when these events occur in the order shown:

1. One of these changes occurs:

- An annotation is added with the same name to a given object on each of two systems in a replication topology, but the annotation has different content on the two systems.

The addition of an annotation to a given object on only one of the systems does not result in a custom metadata collision if the object does not have an annotation with the same name on the other system. In this case, the new annotation is replicated without conflict.

- Different changes are made to the content of a given annotation for a given object on each of the two systems in a replication topology.
- A change is made to the content of a given annotation for a given object on one system in a replication topology, and the same annotation is deleted on another system in the topology.

2. The change made on one of the systems is replicated to the other system.

If a collision occurs when a custom metadata change for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- If the last change on system A is more recent than the last change on system B, HCP applies the change from system A to the custom metadata on system B
- If the last change on system B is more recent than the last change on system A, HCP does not change the custom metadata on system B

Here are two examples of how HCP handles collisions when custom metadata changes for a given object are replicated from one system (system A) in a replication topology to another system (system B) in the topology.

### Example 1

The object starts out with annotations named a1 and a2 on both system A and system B.

The table below shows a sequence of events in which the annotations for the object are changed and the changes are then replicated.

Sequence	Event
1	On system B, a client changes the content of a1.
2	On system A, a client makes a different change to the content of a1.
3	On system A, a client adds annotation a3 to the object.
4	On system B, a client adds annotation a3 with different content from the a3 added on system A.
5	<p>The changes on system A are replicated to system B. The resulting annotations for the object on system B are:</p> <p>a1 with the changed content from system A  a2 (unchanged)  a3 with the content added on system B</p>
6	<p>The changes on system B are replicated to system A. The resulting annotations for the object on system A are:</p> <p>a1 with the changed content from system A  a2 (unchanged)  a3 with the content added on system B</p>

### Example 2

The object starts out with the annotations named a1, a2, and a3 on both system A and system B.

The table below shows a sequence of events in which the annotations for the object are changed and the changes are then replicated.

Sequence	Event
1	On system B, a client changes the content of a1.
2	On system A, a client deletes a1.
3	On system A, a client changes the content of a2.
4	On system B, a client changes the content of a2.
5	On system A, a client deletes a3.
6	On system B, a client changes the content of a3.
7	<p>The changes on system A are replicated to system B. The resulting annotations for the object on system B are:</p> <p>a2 with the changed content from system B  a3 with the changed content from system B</p>



*(Continued)*

Sequence	Event
8	<p>The changes on system B are replicated to system A, the resulting annotations for the object on system A are:</p> <p>a2 with the changed content from system B a3 with the changed content from system B</p>

## Access control list collisions

An ACL collision occurs when these events occur in the order shown:

1. Different changes are made to the ACL for a given object on each of two systems in a replication topology.
2. The changed ACL on one of the systems is replicated to the other system.

An ACL is treated as a single unit. If a collision occurs when a changed ACL for a given object is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- If the last change to the ACL on system A is more recent than the last change to the ACL on system B, HCP changes the ACL on system B to match the changed ACL on system A
- If the last change to the ACL on system B is more recent than the last change to the ACL on system A, HCP does not change the ACL on system B

For example, suppose the ACL for a given object starts out with these grants on both system A and system B:

All users: read  
User lgreen: write  
User mwhite: write, delete

The table below shows a sequence of events in which the ACL for the object is changed and the change is then replicated.

Sequence	Event
1	<p>On system B, a client changes the grants in the ACL to:</p> <p>All users: read User lgreen: write, delete User mwhite: write, delete, read ACL</p>

*(Continued)*

Sequence	Event
2	On system A, a client changes the grants in the ACL to:  All users: read User mwhite: write User pdgrey: write
3	The changed ACL on system A is replicated to system B. The resulting ACL for the object on system B contains these grants:  All users: read User mwhite: write User pdgrey: write

## Configuration collisions

A configuration collision occurs when these events occur in the order shown:

1. Different changes are made to the same configuration property on each of two systems in a replication topology.
2. The changed property on one of the systems is replicated to the other system.

Examples of configuration properties are:

- The data access permission mask for a namespace
- The default shred setting for a namespace
- The HTTP protocol enabled setting for a namespace
- The default versioning setting for new namespaces
- The roles for a user account
- The data access permissions a group account has for a namespace
- The protocol optimization setting on a namespace

Certain groups of properties are treated as a single unit. Generally, these groups consist of properties that are updated by a single submission in the Tenant Management Console. Two notable exceptions to this rule are data access permissions for user accounts and content properties for content classes. In these cases, each set of data access permissions for a namespace and each content property is treated as an individual property.

If a collision occurs when a configuration change is replicated from one system (system A) in a replication topology to another system (system B) in the topology:

- If the last change to the configuration on system A is more recent than the last change to the configuration on system B, HCP changes the configuration on system B to match the configuration on system A
- If the last change to the configuration on system B is more recent than the last change to the configuration on system A, HCP does not change the configuration on system B

The rules above apply to all configuration collisions except collisions that occur when retention class properties are changed. For information on how HCP handles this type of collision, see [“Retention class collisions”](#) below.

Here are two examples of how HCP handles collisions when configuration changes are replicated from one system (system A) in a replication topology to another system (system B) in the topology.

#### Example 1

A given namespace starts out on both system A and system B with these properties:

Read from remote system: enabled  
Collision handling: move object

The table below shows a sequence of events in which the namespace configuration is changed and the change is then replicated.

Sequence	Event
1	On system B, an administrator disables read from replica for the namespace.
2	On system A, an administrator changes the collision handling option for the namespace to rename object.
3	<p>The change on system A is replicated to system B. Because read from remote system and collision handling are properties in the same submission group, the resulting properties for the namespace on system B are:</p> <p>Read from remote system: enabled Collision handling: rename object</p>

**Example 2**

A given user account starts out on both system A and system B with these roles and data access permissions:

Roles: monitor, compliance

Namespace-1 permissions: browse, read, write, delete

The table below shows a sequence of events in which the user account is changed and the changes are then replicated.

Sequence	Event
1	On system B, a security administrator adds the administrator role to the user account.
2	On system A, a security administrator removes the monitor role from the account.
3	On system B, an administrator removes the write permission from Namespace-1 and adds the purge permission.
4	On system A, an administrator adds the privileged permission to Namespace-1.
5	On system B, an administrator gives the user account browse and read permissions for Namespace-2.
6	On system A, an administrator gives the user account browse, read, and write permissions for Namespace-3.
7	<p>The changes on system A are replicated to system B. Because roles and data access permissions are in separate submission groups, the resulting roles and data access permissions for the user account on system B are:</p> <p>Roles: compliance  Namespace-1 permissions: browse, read, write, delete, privileged  Namespace-2 permissions: browse, read  Namespace-3 permissions: browse, read, write</p>

**Retention class collisions**

A retention class collision occurs when these events occur in the order shown:

1. Different changes are made to the same retention class on each of two systems in a replication topology.
2. The changed retention class on one of the systems is replicated to the other system.

If a collision occurs when a change to a retention class is replicated from one system (system A) in a replication topology to another system (system B) involved in the topology:

- **If the last change to the retention class on system A is more recent than the last change to the class on system B and:**
  - The value of the class on system A is greater than the value of the class on system B, HCP changes the value of the class on system B to the value of the class on system A
  - The value of the class on system A is less than the value of the class on system B and:
    - System B is in enterprise mode, HCP changes the value of the class on system B to the value of the class on system A



**Note:** An exception to this rule is when the value of the class on system A is -2 (Initial Unspecified) and the value of the class on system B is *not* 0 (Deletion Allowed). In this case, the value of the class on system B does not change.

---

- System B is in compliance mode, HCP does not change the value of the class on system B
- **If the last change to the retention class on system B is more recent than the last change to the class on system A**, HCP does not change the value of the class on system B



**Note:** A retention class value of -1 (Deletion Prohibited) is greater than a value that's a specific duration. A retention class value of 0 (Deletion Allowed) or -2 (Initial Unspecified) is less than a value that's a specific duration.

---

## Service plans

A **service plan** is a named option that can be associated with a namespace. This option determines how HCP manages the objects in that namespace. Service plan names are system specific.

When creating a tenant, the HCP system administrator specifies whether the tenant is allowed to associate service plans with namespaces. HCP system administrators can change this setting from not allowing these associations to allowing them. However, they cannot do the reverse.

The service plan you select for a namespace should match the expected usage pattern and properties for that namespace. For example, if the purpose of the namespace is to store objects that most likely will not be accessed again, you would choose a service plan with a description indicating that the plan is intended for archiving.

## System-level administrative access

A tenant can optionally grant HCP system-level users administrative access to itself. This enables those users to access the Tenant Management Console for that tenant and perform the same management and monitoring activities as the tenant-level users. Additionally, it enables system-level users to search the namespaces owned by that tenant and perform all allowed operations on the objects they find.

For more information on system-level administrative access to tenants, see [“Enabling or disabling system-level administrative access”](#) on page 104. For information on the Tenant Management Console, see [“Tenant Management Console”](#) on page 48.

# General administrative information

As an HCP tenant administrator, you are responsible for managing a tenant and the namespaces it owns. Your primary job is to ensure that users and applications have the access they need to those namespaces.

The tool you use for this purpose is a web application called the **Tenant Management Console**. Depending on the permissions you have, you can use the Console to configure and monitor the tenant and its namespaces, as well as perform compliance activities.

This chapter:

- Presents basic information about using the Tenant Management Console
- Describes your responsibilities as a tenant administrator

## Tenant Management Console

The Tenant Management Console is a tenant-specific web application that lets you manage tenants and namespaces. The Console shows you tenant and namespace status in real time, so you can effectively monitor activity and take action as needed.

Using the Console, you can modify tenant and namespace settings and perform compliance activities. Changes you make through the Console take effect immediately.

Access to the Tenant Management Console is available only through HTTP with SSL security (HTTPS).

### Console access

To use the Tenant Management Console, you need either:

- A user account defined in HCP (either locally authenticated or RADIUS authenticated).
- If the tenant is configured to support Windows Active Directory (AD) authentication, an AD user account for a user that belongs to one or more AD groups for which corresponding group accounts are defined in HCP. In this book, such an Active Directory user account is referred to as a **recognized AD user account**.

The HCP user account or group accounts specify what you have permission to do in the Console. The menu options, pages, and panels you see in the Console depend on your permissions.

If an AD user belongs to multiple AD groups for which HCP group accounts exist, that user has all the permissions associated with all those group accounts.

For more information on user and group accounts, see [“About user and group accounts”](#) on page 62.

### Console sessions

A Tenant Management Console session begins when you do one of these:

- Log into the Console using an HCP user account or recognized AD user account.
- Access a Console page while logged into Windows with a recognized AD user account. This is called **single sign-on**. With single sign-on, you don't need to explicitly log into the Console.



For single sign-on to work, your web browser must be configured to support it. For more information on this, see [Appendix C, “Browser configuration for single sign-on with Active Directory.”](#) on page 269.

A session ends when you log out. During a session, you can perform any actions for which you have permission.

During a session, if you don't take any action for a certain amount of time, the Console displays the **Idle Timeout** page. If you explicitly logged into the session, the Console automatically logs you out and, when you click on any tab on the **Idle Timeout** page, displays the login page. If you started the session by using single sign-on, when you click on any tab, the Console displays the requested page. The exact amount of idle time allowed is configurable. For information on setting this value, see [“Changing user account and login settings”](#) on page 90.

If you've granted HCP system-level users administrative access to the tenant, they can access the Tenant Management Console directly from the HCP System Management Console. Doing so does not start a Tenant Management Console session. Rather, it continues the current System Management Console session, and the configured idle time for that Console applies.

For information on granting this access, see [“Enabling or disabling system-level administrative access”](#) on page 104.

### HCP management API

HCP includes a RESTful HTTP interface to a subset of its administrative functions. Using this interface, called the **management API**, you can modify your tenant and create, modify, and delete namespaces, user and group accounts, and content classes for the tenant. Additionally, you can create, modify, and delete retention classes for namespaces owned by the tenant.

You use the Tenant Management Console to enable the management API at the tenant level. For the API to be available, however, it must also be enabled at the system level.

To use the management API, you need a user account that includes the applicable permissions for the actions you want to take.

If the tenant is configured to support Active Directory authentication, applications can also use recognized AD user accounts to access HCP through the management API. To do this, however, an application must use the SPNEGO protocol to negotiate the AD user authentication itself. For more information on SPNEGO, see <http://tools.ietf.org/html/rfc4559>.

For information on enabling the management API, see [“Controlling access to HCP through the management API”](#) on page 106. For information on using the HCP management API, see *HCP Management API Reference*.

## Tenant Management Console URL

The URL for the Tenant Management Console has this format:

```
https://tenant-url-name.hcp-domain-name:8000
```

For example, to access the Tenant Management Console for the tenant named Finance in the HCP system with the domain name hcp-ma.example.com, you would use this URL:

```
https://finance.hcp-ma.example.com:8000
```

### Using a hosts file

Typically, the HCP system uses DNS for system addressing. If this is not the case, you need to provide a mapping of the tenant hostname to an IP address for the HCP system.

You specify hostname mappings in the `hosts` file on the client. The location of this file depends on the client operating system:

- On Windows, by default: `c:\windows\system32\drivers\etc\hosts`
- On Unix: `/etc/hosts`
- On Mac OS® X: `/private/etc/host`

### Hostname mappings

Each entry in a `hosts` file maps one or more fully qualified hostnames to a single IP address. For example, if one of the IP addresses for the HCP system is 192.168.210.16, you would add this line to the `hosts` file on the client to enable access to the Tenant Management Console for the Finance tenant:

```
192.168.210.16    finance.hcp-ma.example.com
```

The following considerations apply to `hosts` file entries:

- Each entry must appear on a separate line.
- Multiple hostnames in a single line must be separated by white space. With some versions of Windows, these must be single spaces.

- Each hostname can map to multiple IP addresses.

You can include comments in a `hosts` file either on separate lines or following a mapping on the same line. Each comment must start with a number sign (`#`). Blank lines are ignored.

For the IP addresses for the HCP system, contact your HCP system administrator.

### Hostname mapping considerations

An HCP system has multiple IP addresses. You can map the tenant hostname to more than one of these IP addresses in the `hosts` file. The way multiple mappings are used depends on the client platform. For information on how your client handles multiple mappings in a `hosts` file, see your client documentation.

If any of the IP addresses listed in the `hosts` file are unavailable, timeouts may occur when you use a `hosts` file to access the Tenant Management Console.

## Logging in

Depending on the tenant configuration, you can log into the Tenant Management Console with a tenant-level user account or a recognized AD user account. For the user account to use when first logging into the Console for a new tenant, see [“Starter account”](#) on page 73.

To log into the Tenant Management Console:

1. Open a web browser.
2. In the address field, enter the URL for your Tenant Management Console.




---

**Note:** If you inadvertently use *http* instead of *https* in the URL, the browser returns an error. Enter the URL again, this time using *https*.

---

One of these happens:

- If all of these are true, you are automatically logged into the Tenant Management Console, and the tenant **Overview** page appears:
  - You are currently logged into Windows with a recognized AD user account.
  - The tenant is configured to support AD authentication.

- Your web browser is configured to support single sign-on with AD. For information on this, see [Appendix C, “Browser configuration for single sign-on with Active Directory.”](#) on page 269.

This is single sign-on. No further action is required.

- If the tenant is configured to support AD authentication but any of the following apply, a message appears indicating that single sign-on was not possible:
  - Your web browser is not configured to support single sign-on.
  - You are not currently logged into Windows with a recognized AD user account.
  - You are not on a Windows computer.

In these cases, you need to click on the **Console login page** link in the message to display the Tenant Management Console login page.

- If the tenant is not configured to support AD authentication, the Tenant Management Console login page appears.



**Note:** The Tenant Management Console login page shows the specific version of the HCP release. Once you enter the Console, the version number appears at the bottom of each page.

---

3. In the **Username** field, type your username.
4. In the **Password** field, type your case-sensitive password.

When using an HCP user account, if you try to log in with an invalid password multiple times in a row, you are locked out of the Console. The exact number of times is configurable. For information on setting this value, see [“Changing user account and login settings”](#) on page 90.



**Note:** AD can also be configured to disable user accounts after a given number of authentication attempts with an invalid password.

---



**Important:** You should change your password as soon as possible the first time you log into the Tenant Management Console.

---

5. If the tenant is configured to support AD authentication, do either of these in the **Domain** field:
  - If you're using an HCP user account, select the domain name of the HCP system.
  - If you're using a recognized AD user account, select the AD domain in which your user account is defined.

If HCP is not configured to support AD, the login page does not display the **Domain** field.

6. Click on the **Log In** button.

The Console displays the tenant **Overview** page or, if you're using an HCP user account and are required to change your password, the **Change Password** page.

For information on the tenant **Overview** page, see ["About the tenant Overview page"](#) on page 96. For information on changing your password, see ["Changing your password"](#) on page 55.

## Using the Tenant Management Console

Tenant Management Console pages display information about the current tenant and its namespaces. Some pages also let you configure various aspects of the tenant and namespaces. (The **current tenant** is the one for which you're currently logged into the Tenant Management Console.)

Console pages have menus and hyperlinks for navigation. Each page shows a horizontal menu at the top. Some of the menu options display a secondary menu when you mouse over them. To navigate to a page, you click on the corresponding menu option.

You can also use shortcut keys to navigate to pages in the Tenant Management Console. Each link that has a shortcut key has the applicable letter underlined. To use the shortcut key, follow the convention for the browser you're using.

Each page of the Tenant Management Console shows the username of the currently logged-in user in the upper right corner.



#### Notes:

- If you're an AD user and your username changes in AD while you're using the Tenant Management Console, the Console may not reflect the new username until you log out and back in. If you're currently using any other HCP interfaces, you need to log out of those as well.
- While the HCP system is experiencing a heavy load, the Tenant Management Console may be slower to present certain information.

## Refreshing pages

Tenant Management Console pages do not automatically refresh themselves while they remain open. To see the most recent values on a page, click again on the menu option that opens that page.



**Note:** Using the browser reload button to refresh a page that lets you create or modify an entity causes the Console to resubmit values you previously entered on the page.

## Submitting changes

Tenant Management Console pages and panels on which you can modify information have action buttons (such as **Create Retention Class** and **Update Settings**) that submit your changes. Action buttons make the changes on a page permanent. These changes take effect immediately.


You need to submit the changes you make before switching to a different page or panel. If you switch without submitting those changes, the Console does not retain them.

For some checkbox options, selecting or deselecting the checkbox causes that change to take effect immediately.

After you submit changes, the Console displays a message indicating whether HCP successfully made the changes. To hide the message, click on **Dismiss** in the message area.

## Viewing HCP documentation

HCP documentation is available online in PDF format. To view a document from the Tenant Management Console:

1. In the top right corner of the Tenant Management Console window, mouse over the documentation icon (  ) to open a dropdown menu of the available documents.
2. In the dropdown menu, click on the document you want.

## Changing your password

Depending on how your user account is set up, HCP may authenticate your username and password locally or remotely when you log in. If your account is set up for local authentication, you can change your password in the Tenant Management Console. When you change your password in this Console, it also changes for any other HCP interfaces to which your user account gives you access.

If your account is set up for remote authentication or if you use an AD user account to access the Console, you use a method outside HCP to change your password.

For information on local and remote authentication, see [“User authentication”](#) on page 70.

To change your locally authenticated password in the Tenant Management Console:

1. Log into the Tenant Management Console using your existing password.
2. In the top right corner of the Console window, click on the **Password** link.
3. On the **Change Password** page:
  - In the **Existing Password** field, type your current password.
  - In the **New Password** field, type your new password. Passwords can be up to 64 characters long, are case sensitive, and can contain any valid UTF-8 characters, including white space.

To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.

The minimum length for passwords is tenant specific. Typically, it's six or eight characters. For information on changing the minimum length for passwords, see ["Changing user account and login settings"](#) on page 90.

When changing your password, you cannot reuse your current password.

- In the **Confirm New Password** field, type your new password again.
4. Click on the **Update Password** button.

## Logging out

To log out of the Tenant Management Console:

1. In the top right corner of the Console window, click on the **Log Out** link.
2. If you explicitly logged in, close the browser window to ensure that other users cannot go back into the Tenant Management Console using the credentials you used to log in.



---

**Tip:** For extra security, clear the browser cache before closing the window.

---

## Administrative responsibilities

Tenant-level administrative responsibilities consist of:

- Managing user and group accounts
- Maintaining the tenant
- Creating and maintaining namespaces
- Monitoring the tenant and namespaces
- Managing namespace access
- Performing compliance activities

You perform these activities in the HCP Tenant Management Console. For information on using this Console, see ["Tenant Management Console"](#) on page 48.



**Managing user and group accounts**

HCP user and group accounts determine whether you can log into the HCP Tenant Management Console or Search Console and which operations you can perform in namespaces. For the Tenant Management Console, they also determine which actions you're allowed to perform after logging in.

You use the Tenant Management Console to create, modify, and delete user and group accounts. For each HCP user account, you specify whether it's authenticated locally or by RADIUS.

You also use the Tenant Management Console to configure login settings for the Console as a whole.

For information on managing user and group accounts and configuring login settings, see [Chapter 4, "Managing accounts."](#) on page 61.

**Maintaining the tenant**

HCP system-level administrators create tenants and maintain certain aspects of their configuration. Other aspects of tenant configuration, however, are maintained at the tenant level.

As a tenant administrator, you are responsible for configuring:

- Tenant contact information
- The tenant description
- The tenant permission mask
- System-level administrative access to the tenant
- Access to the Tenant Management Console
- Access to HCP through the management API
- Access to the Search Console for the tenant

For information on these activities, see ["Configuring the tenant"](#) on page 101.

You are also responsible for creating and managing content classes and content properties for the tenant. For information on this, see [Chapter 8, "Managing search and indexing."](#) on page 203.

### Creating and maintaining namespaces

As a tenant administrator, you are responsible for creating and maintaining namespaces. After creating a namespace, you can change most of its properties. You are also responsible for managing search and indexing for the namespace.

In addition to creating and modifying namespaces, you can delete them, but only if they don't contain any objects.

For information on:

- Creating namespaces, see ["Creating a namespace"](#) on page 144
- Changing namespace properties, see ["Configuring a namespace"](#) on page 149 and ["Selecting or deselecting namespaces for replication"](#) on page 125
- Managing search and indexing, see [Chapter 8, "Managing search and indexing for an individual namespace,"](#) on page 236
- Deleting namespaces, see ["Deleting a namespace"](#) on page 177



---

**Note:** Users with the allow namespace management property can use the HCP management and HS3 APIs to create, view and change the versioning status of, and delete namespaces.

---

### Monitoring the tenant and namespaces

HCP is a self-monitoring, self-healing system that automatically alerts you to any issues you may need to address (such as a namespace running low on space). The Tenant Management Console enables you to review tenant and namespace activity and take action to address certain issues. Using the Console, you can view:

- Statistics and graphs showing namespace usage. For more information on this, see:
  - ["Tenant statistics"](#) on page 96
  - ["Objects section"](#) on page 140
  - ["Usage section"](#) on page 141

- Messages about tenant and namespace events, such as configuration changes and searches performed from the Search Console. For information on this, see:
  - [“Major tenant events”](#) on page 97
  - [“Viewing the complete tenant event log”](#) on page 109
  - [“Major namespace events”](#) on page 142
  - [“Viewing the complete namespace event log”](#) on page 174
- Messages about security events (that is, attempts to log into the Tenant Management Console with an invalid username). For information on this, see [“Viewing the tenant security log”](#) on page 110.
- Messages about compliance events (that is, retention class activity and privileged delete operations). For information on this, see:
  - [“Viewing the tenant compliance log”](#) on page 110
  - [“Viewing the namespace compliance log”](#) on page 175
- Reports of irreparable objects. For information on this, see [“Working with irreparable objects”](#) on page 175.
- Alerts warning you of conditions that may need your attention. For information on this, see:
  - [“Tenant alerts”](#) on page 98
  - [“Namespace alerts”](#) on page 142
- The progress of replication activity. For information on this, see [“Monitoring and managing replication”](#) on page 121.

You can also have HCP send tenant and namespace log messages to syslog servers, SNMP managers, and specified email addresses. For information on this see:

- [“Enabling syslog logging”](#) on page 113
- [“Enabling SNMP logging”](#) on page 113
- [“Configuring email notification”](#) on page 114

Additionally, you can generate chargeback reports that can be used as input to billing applications. For information on this, see [“Generating chargeback reports”](#) on page 127.

### **Managing namespace access**

Managing namespace access entails:

- Setting the tenant and namespace data access permission masks (see [“Changing the tenant permission mask”](#) on page 103 and [“Changing the namespace permission mask”](#) on page 151)
- Setting minimum data access permissions for authenticated and unauthenticated users (see [“Changing minimum data access permissions”](#) on page 159)
- Configuring the namespace access protocols for client access to each namespace (see [Chapter 7, “Configuring namespace access protocols,”](#) on page 179)
- Optionally, setting the IP addresses from which access to the Search Console is allowed or denied (see [“Controlling access to the Search Console”](#) on page 107)
- Optionally, downloading HCP Data Migrator for installation on client computers (see [Chapter 11, “Downloading HCP Data Migrator,”](#) on page 251)

### **Performing compliance activities**

The Tenant Management Console enables you to perform certain activities required for compliance with some local regulations. Using the Console, you can:

- Create, modify, and delete retention classes (see [Chapter 9, “Working with retention classes,”](#) on page 241)
- Perform privileged delete operations (see [Chapter 10, “Using privileged delete,”](#) on page 247)

## Managing accounts

As a tenant security administrator, you are responsible for creating and managing tenant-level user and group accounts. These accounts give users permission to use the Tenant Management Console and HCP management API and to access namespace content through namespace access protocols that require authentication, the Namespace Browser, the HCP metadata query API, and the HCP Search Console. These accounts also determine which actions the user is allowed to perform through the applicable interface.

Users with HCP user accounts are authenticated locally by HCP or remotely by RADIUS. Group accounts enable users defined in Active Directory to access HCP interfaces. These users are authenticated remotely by AD. The tenant configuration determines which types of authentication the tenant supports.

As an administrator with the security role, you can associate administrative roles with user and group accounts. To associate data access permissions with user and group accounts, you need the administrator role.

Different tenants have different user and group accounts. These accounts cannot be shared across tenants.

This chapter explains how to:

- Create and manage user and group accounts
- Change Tenant Management Console login settings

For an introduction to the Tenant Management Console, see [“Tenant Management Console”](#) on page 48.

## About user and group accounts

User and group accounts control access to HCP interfaces. The administrative roles associated with these accounts allow users to use:

- The Tenant Management Console
- The HCP management API

You need the security role to create, modify, delete, and associate roles with user and group accounts.

The data access permissions associated with user and group accounts allow users to access namespace content through:

- Namespace access protocols that require authentication
- The Namespace Browser
- The HCP metadata query API
- The HCP Search Console

You need the administrator role to associate data access permissions with user and group accounts.

The allow namespace management property, which you can assign to a user or group account, allows users to use the HCP management and HS3 APIs to:

- Create namespaces
- List, view and change the versioning status of, and delete namespaces they own

You need the administrator role to assign the allow namespace management property to a user or group account.

### User accounts

An HCP user account is a set of credentials that gives a user access to one or more of the interfaces listed above. You create and manage user accounts in the Tenant Management Console.

When you create a user account, you specify whether the user credentials are authenticated locally or by RADIUS. Additionally, for locally authenticated users, you specify whether the account password must be changed the next time the account is used to access one of the Consoles.

When you create a user account, you have the option of associating roles with it and assigning the allow namespace management property. You can change these properties as well associate data access permissions with the account at any time thereafter.

You can enable and disable user accounts, as needed. While an account is disabled, it cannot be used to access any of the applicable interfaces. You might decide to disable an account, for example, while the user for whom you created it is on vacation.

Multiple people can use the same user account concurrently for the same or different interfaces. To prevent this from happening, you should create a separate account for each user, and users should keep their passwords confidential.



---

**Note:** For HCP user accounts, HCP logs failed namespace access attempts with a given username once an hour. This prevents repeated log messages in the case where an application specifies invalid credentials. The message that's logged indicates the number of failed attempts that occurred in the past hour.

---

A tenant can have at most 10,000 HCP user accounts.

### Group accounts

An HCP group account is a representation of an Active Directory group. The group account enables AD users in the AD group to access one or more of the interfaces listed in [“About user and group accounts”](#) on page 62. You create and manage group accounts in the HCP Tenant Management Console.

When you create a group account, you have the option of associating roles with it. You can change these associations and also associate data access permissions with the account at any time thereafter.

A tenant can have at most 100 group accounts.

## Administrative roles and permissions

A **role** is a named collection of permissions that can be granted to a user either through an HCP user account or through one or more HCP group accounts. Each permission in a role lets the user perform some specific interaction or set of interactions with the HCP system. Roles generally correspond to job functions.

You can associate any number of roles with a user or group account. The account user then has all the permissions granted by each of those roles.



---

**Tip:** Before associating roles with a user or group account, make sure the permissions granted by those roles are consistent with job functions of the user or group for which you're creating the account.

---



---

**Note:** An AD user can be added to an AD group while that user is using the Tenant Management Console. If the AD group corresponds to an existing HCP group account, the user may not automatically get the roles associated with that group account for up to eight hours. To get the roles immediately, the user needs to log out of the Tenant Management Console and then log back in. If the user is also currently using the HCP System Management Console or the Namespace Browser, logging out of either of those interfaces has the same effect.

---

### Available roles

The roles you can associate with a user or group account are:

- **Monitor** — Grants permission to use the Tenant Management Console to view the status of the tenant and its namespaces and most aspects of the tenant and namespace configurations. The monitor role does not grant permission to view user or group accounts.
- **Administrator** — Grants permission to use the Tenant Management Console to view the status of the tenant and its namespaces and perform most tenant and namespace configuration activities. The administrator role also grants permission to associate data access permissions with user and group accounts but not to view or manage any other aspects of user and group accounts.
- **Security** — Grants permission to use the Tenant Management Console to view the status of the tenant, configure Console and HCP management API security, and view security events in the tenant log.



The security role also grants permission to create and manage user and group accounts, including associating roles with them but not viewing or managing their data access permissions.

- **Compliance** — Grants permission to use the Tenant Management Console to work with retention classes and retention-related settings and perform privileged deletes, as well as to view tenant status, namespace status, and compliance events in the tenant log.

## Permissions granted by roles

In the table below, checkmarks indicate the permissions granted by each role.

Permission	Role			
	Monitor	Administrator	Security	Compliance
View the user account list	✓	✓	✓	
View the full definition of individual user accounts			✓	
View the description, allow namespace management property, and data access permissions for individual user accounts	✓	✓		
Create, associate roles with, delete, and otherwise manage user accounts, except modifying the allow namespace management property and data access permissions			✓	
Modify the allow namespace management property and manage data access permissions for user accounts		✓		
View the group account list	✓	✓	✓	
View the full definition of individual group accounts			✓	
View the description, allow namespace management property, and data access permissions for individual group accounts	✓	✓		
Create, associate roles with, and delete group accounts			✓	
Modify the allow namespace management property and manage data access permissions for group accounts		✓		
Specify message text for the Tenant Management and Search Console login pages			✓	
View the tenant overview	✓	✓	✓	✓
Modify the tenant contact information, permission mask, and description		✓		

*(Continued)*

Permission	Role			
	Monitor	Administrator	Security	Compliance
Allow or disallow access to the Tenant Management Console by HCP system-level users		✓		
View and modify Tenant Management Console security settings			✓	
View and modify HCP management API security settings			✓	
View and modify Search Console security settings			✓	
View content classes and content properties	✓	✓		
Create, modify, and delete content classes and content properties		✓		
View namespace associations with content classes	✓	✓		
Modify namespace associations with content classes		✓		
View tenant log messages about all events except compliance and security events	✓	✓	✓	✓
View tenant log messages about compliance events				✓
View tenant log messages about security events			✓	
View syslog and SNMP logging options	✓	✓		
Enable or disable syslog and SNMP logging		✓		
View email notification settings	✓	✓		
Modify email notification settings		✓		
Generate chargeback reports	✓	✓		
Create and delete namespaces		✓		
View the namespace list	✓	✓		✓
View namespace overviews	✓	✓		✓
Modify namespace names and quotas		✓		
View namespace permission masks and descriptions	✓	✓		✓
Modify namespace permission masks and descriptions		✓		
View namespace owners	✓	✓		✓
Change namespace owners		✓		
View the tags associated with namespaces	✓	✓		

*(Continued)*

Permission	Role			
	Monitor	Administrator	Security	Compliance
Modify the tags associated with namespaces		✓		
View namespace default retention settings	✓	✓		✓
Modify namespace default retention settings				✓
View namespace default shred settings	✓	✓		✓
Modify namespace default shred settings				✓
View namespace default index settings	✓	✓		
Modify namespace default index settings		✓		
View minimum data access permissions	✓	✓		
Modify minimum data access permissions		✓		
View namespace ACL settings (HCP tenants only)	✓	✓		
Manage the use of ACLs in namespaces		✓		
View namespace retention-related settings	✓	✓		✓
Modify namespace retention-related settings				✓
View the custom metadata XML checking setting for namespaces	✓	✓		
Modify the custom metadata XML checking setting for namespaces		✓		
View namespace object versioning configurations	✓	✓		
Configure object versioning in namespaces		✓		
View namespace compatibility settings	✓	✓		
Modify namespace compatibility settings		✓		
View namespace disposition settings	✓	✓		✓
Modify namespace disposition settings				✓
View namespace replication-related settings	✓	✓		
Modify namespace replication-related settings		✓		
View the service plans associated with namespaces	✓	✓		
Associate service plans with namespaces		✓		
View namespace DPL settings	✓	✓		

*(Continued)*

Permission	Role			
	Monitor	Administrator	Security	Compliance
Modify namespace DPL settings		✓		
View namespace retention modes	✓	✓		
Modify namespace retention modes		✓		
View default settings for namespace creation	✓	✓		
Modify default settings for namespace creation		✓		
View the maximum number of namespaces per user	✓	✓		
Modify the maximum number of namespaces per user		✓		
View namespace access protocol configurations	✓	✓		
Configure namespace access protocols for namespaces		✓		
View search and indexing options for namespaces	✓	✓		
Modify search and indexing options for namespaces		✓		
Reindex namespaces		✓		
Monitor replication	✓	✓		
Select namespaces for replication		✓		
View all namespace log messages except messages about compliance events	✓	✓	✓	✓
View namespace log messages about compliance events				✓
View the list of irreparable objects	✓	✓		
Acknowledge irreparable objects		✓		
Create, modify, and delete retention classes				✓
View the list of retention classes	✓	✓		✓
View individual retention classes	✓	✓		✓
Perform privileged delete operations				✓
Download HCP Data Migrator	✓	✓	✓	✓
Change your own locally authenticated password in the Tenant Management Console	✓	✓	✓	✓
View HCP documentation from the Tenant Management Console	✓	✓	✓	✓

## Data access permissions

Data access permissions allow users to access namespace content and some information about namespaces. These permissions are namespace specific. That is, they are granted separately for individual namespaces.

The data access permissions that can be associated with user and group accounts for any given namespace are:

- **Browse** — Lets users list directory contents.
- **Read** — Lets users:
  - View and retrieve objects, including the system and custom metadata for objects
  - View and retrieve previous versions of objects
  - Check the existence of objects
  - List annotations for objects

For this permission to be granted, users must also have browse permission.

- **Read ACL** — Lets users view and retrieve object ACLs.
- **Write** — Lets users:
  - Add objects to the namespace
  - Modify system metadata (except retention hold)
  - Add or replace custom metadata
- **Write ACL** — Lets users add, replace, and delete object ACLs.
- **Change owner** — Lets users change the owners of objects in the namespace.
- **Delete** — Lets users delete objects, custom metadata, and ACLs from the namespace.
- **Purge** — Lets users delete all versions of an object with a single operation. For this permission to be granted, users must also have delete permission.

- **Privileged** — Lets users:
  - Delete or purge objects that are under retention, provided that the user also has delete or purge permission for the applicable namespace
  - Hold or release objects, provided that the user also has write permission for the applicable namespace
- **Search** — Lets users use the HCP metadata query API and the HCP Search Console to query or search the namespace. For this permission to be granted, users must also have read permission.

Users with any data access permissions for a namespace can view information about that namespace.



---

**Note:** An AD user can be added to an AD group while that user is using the Namespace Browser. If the AD group corresponds to an existing HCP group account, the user may not automatically get the data access permissions associated with that group account for up to eight hours. To get the data access permissions immediately, the user needs to log out of the Namespace Browser and then log back in. If the user is also currently using the HCP System Management Console or the Tenant Management Console, logging out of either of those interfaces has the same effect.

---

## User authentication

To use these HCP Console and command-line interfaces, a user needs to supply a username and password for authentication:

- Console interfaces:
  - Tenant Management Console
  - Namespace Browser
  - HCP Search Console
- Command-line interfaces:
  - HCP management API
  - Namespace access protocols that require authentication
  - HCP metadata query API

**User authentication** is the process of checking whether the combination of the specified username and password is valid.

For user accounts defined in HCP, the system supports local and RADIUS authentication. User accounts defined in AD must be authenticated by AD. RADIUS and AD authentication are types of **remote authentication**.

A tenant can support one or more of these authentication types. The types supported are set when the tenant is created. HCP system-level administrators can change these settings at any time.

### Local authentication

For locally authenticated users, the user account password is stored in the HCP system. When a user submits the account username and password either on a login page for a Console or with a cookie in a command line, HCP checks the username and password internally.

HCP lets the user into the target Console or performs the requested operation if these conditions are true:

- The combination of the specified username and password is valid.
- The user account is enabled.
- For the Tenant Management Console, the user account is associated with at least one role.
- For the Search Console, the user account is associated with the search permission.
- For the HCP management API, the user account is associated with a role that allows the requested operation.
- For a namespace access protocol, the user account is associated with permissions that allow the requested operation.
- For the metadata query API, the user account is associated with the search permission.

If any of these conditions is not true, HCP rejects the login or command-line request.

You can change the passwords of locally authenticated users in the Tenant Management Console. These users can also change their own passwords in the Tenant Management Console, if they have access to it, or in the Search Console, if they have access to that.

### **RADIUS authentication**

For RADIUS-authenticated users, the user account password is stored outside the HCP system. When a user submits the account username and password either on a login page for a Console or with a cookie in a command line, HCP securely sends the submitted username and password to a RADIUS server. That server checks whether the username and password are valid and sends the result to HCP.

HCP lets the user into the target Console or performs the requested operation if these conditions are true:

- The combination of the specified username and password is valid.
- The user account is enabled.
- For the Tenant Management Console, the user account is associated with at least one role.
- For the Search Console, the user account is associated with the search permission.
- For a command-line interface, the user account is associated with permissions that allow the requested operation.

If any of these conditions is not true, HCP rejects the login or command-line request.

All password management for RADIUS-authenticated users is handled by the RADIUS server. You cannot use the Tenant Management Console to set or change the passwords of RADIUS-authenticated users.

Connections to RADIUS servers are configured at the HCP system level.



---

**Note:** RADIUS authentication is not supported for the namespace access protocols or for access to namespace content through any other interface.

---

### **Active Directory authentication**

For AD-authenticated users, the username and password for the user account are stored in AD. If the user is signed into a Windows client, HCP relies on Windows to have already validated the username and password with AD (this is single sign-on). However, if the user provides an AD username and password on the System Management Console or Search Console login page, HCP securely sends the specified username and password to AD for authentication.



HCP lets an authenticated user into the target Console only if these conditions are true:

- The user belongs to at least one AD group for which a corresponding group account exists in HCP.




---

**Note:** Alternatively, the user can belong to an AD group that's nested at any level under another group for which a corresponding HCP group account exists. In this case, however, any parent groups that are defined in a domain other than the user's domain must be universal.

---

- For the Tenant Management Console, at least one such group account is associated with at least one role.
- For the Search Console, at least one such group account is associated with the search permission.

If any of these conditions is not true, HCP doesn't let the user in.

All password management for AD-authenticated users is handled by AD. You cannot use the Tenant Management Console to set or change the passwords of AD-authenticated users.

For the command-line interfaces, applications must use the SPNEGO protocol to negotiate the AD user authentication themselves. You cannot submit AD credentials with a cookie in a command line. For more information on SPNEGO, see <http://tools.ietf.org/html/rfc4559>.




---

**Note:** AD authentication is not supported for namespace creation through the HS3 protocol.

---




---

**Tip:** If the tenant supports both local and AD authentication, consider creating a locally authenticated user account with the security role. This ensures that you can still access the Tenant Management Console in the unlikely event that HCP cannot communicate with AD.

---

## Starter account

When creating a tenant, the HCP system administrator defines either one locally authenticated HCP user account or one HCP group account for it. This starter account has only the security role and no data access permissions. It also does not have the allow namespace management property.

Before you can log into the Tenant Management Console:

- If the starter account is an HCP user account, you need to get the username and password for this account from the system administrator. The first time you log in with this account, you are immediately required to change your password.
- If the starter account is an HCP group account, you need to get the username and password of an AD user account for a user that belongs to the AD group that corresponds to the starter group account.

After you've logged in with the starter account, you can create new accounts as needed, including new accounts with the security role.

You can delete the starter account as long as at least one of these will still exist after you delete the account:

- A locally authenticated HCP user account that has the security role and is enabled
- An HCP group account that has the security role

## Working with user accounts

To view, create, and manage HCP user accounts, you use the **Users** page in the Tenant Management Console. To display this page:

1. In the top-level menu in the Tenant Management Console, mouse over **Security** to display a secondary menu.
2. In the secondary menu, click on **Users**.




---

**Roles: To:**

- View the user account list, you need the monitor, administrator, or security role
  - View the full definitions of user accounts, you need the security role
  - View the description, allow namespace management property, and data access permissions for user accounts, you need the monitor or administrator role
  - Create, associate roles with, delete, and otherwise manage user accounts, except modifying the allow namespace management property and data access permissions, you need the security role
  - Modify the allow namespace management property and data access permissions for user accounts, you need the administrator role
- 

## About the Users page

The **Users** page lets you create, modify, and delete user accounts. It also lists the existing user accounts. For information on this list, see [“Understanding the user account list”](#) and [“Managing the user account list”](#) below.

### Understanding the user account list

The **Users** page lists existing user accounts. For each account, the list shows:

- The username
- Whether the account is enabled or disabled
- The full name of the account user
- Whether the user login is authenticated locally or by RADIUS

To view additional information about an individual user account, click on the account username.



## Managing the user account list

By default, the user account list on the **Users** page includes all existing user accounts. The accounts are listed 20 at a time in ascending order by username.

You can page through, sort, and filter the list of user accounts. The **Users** page indicates which accounts are shown out of the total number of accounts in the current list.

### Paging

You can change the number of user accounts shown at a time on the **Users** page. To do this, in the **Items per page** field, select the number of tenants you want. The options are 10, 20, and 50.

To page forward or backward through the user account list, click on the next (  ) or back (  ) control, respectively.

To jump to a specific page in the user account list:

1. In the **Page** field, type the page number you want.
2. Press Enter.


### Sorting


You can sort the user account list in ascending or descending order by username. To change the sort order, click on the **Username** column heading. Each time you click on the column heading, the sort order switches between ascending and descending.

### Filtering

You can filter the user account list by username. The filtered list includes only those user accounts with a username that begins with or is the same as a specified text string.

To filter the user account list:

1. In the entry field above the list, type the text string you want to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
2. Click on the find control (  ).

To redisplay the entire list of user accounts after filtering it, click on the clear filter control (  ).

## Creating a user account

To create a user account:

1. On the **Users** page in the Tenant Management Console, click on **Create User Account**.
2. In the **Create User Account** panel:
  - Optionally, deselect the **Enable account** option to have the user account initially disabled.

A disabled user account cannot be used to access the Tenant Management Console or HCP Search Console. It can, however, be used for namespace access with the HTTP protocol and Namespace Browser.

- In the **Username** field, type a login name for the user account. Usernames must be from one through 64 characters long and can contain any valid UTF-8 characters but cannot start with an opening square bracket ([). White space is allowed.

Usernames are not case sensitive.

The username for a user account must be unique for the current tenant. Different tenants can have user accounts with the same username.

You can reuse usernames that are not currently in use. So, for example, if you delete the account for a user, you can create a new account for that user with the same username as before.




---

**Tip:** Consider using email addresses as usernames. This enables users to more easily remember their HCP usernames. It also gives you easy access to email addresses should you need to contact any users.

---

- In the **Full Name** field, type the name of the person for whom you're creating the user account. This name must be from one through 64 characters long and can contain any valid UTF-8 characters, including white space.
- For the **Authentication** option, select either **Local** or, for remote authentication, **RADIUS**.

If you select **Local**, the panel displays the **Password** and **Confirm Password** fields and **Force change on next login** option. If you select **RADIUS**, these fields are hidden.

For local authentication:

- In the **Password** field, type a password for the user account. Passwords can be up to 64 characters long, can contain any valid UTF-8 characters, including white space, and are case sensitive.

To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.

The minimum length for passwords is tenant specific. Typically, it's six or eight characters. For information on changing the minimum length for passwords, see ["Changing user account and login settings"](#) on page 90.



---

**Note:** HCP does not save passwords in a recoverable format. If a user forgets his or her password, you need to assign a new one.

---

- In the **Confirm Password** field, type the password again.
- Optionally, select the **Force change on next login** option.

When this option is selected, the next time a user uses the account to log into the Tenant Management Console, the Console automatically displays the **Change Password** page. The user cannot do anything else in the Console until the password is changed.

Once the user changes the password, the **Force change on next login** option is automatically deselected.

- In the **Roles** section, select any number of roles for the user account, including none. For descriptions of the available roles, see ["Administrative roles and permissions"](#) on page 64.
- Optionally, specify a description for the user account:
  1. Click on **Description**.
  2. In the **Description** field, type a description of the user account. This text can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

- Optionally, if you have the administrator role, select the **Allow namespace management** option. (This option is selected automatically and cannot be deselected if the account being created has the administrator role.)
- Optionally, if you have the administrator role, click on **Assign Namespace Permissions**. Then associate data access permissions with the user account, as described in [“Specifying permissions for any number of namespaces”](#) on page 87.



**Note:** You cannot associate data access permissions with a RADIUS-authenticated user account.

---

3. Click on the **Create User Account** button.

## Modifying a user account and its roles

As a user with the security role, you can change this information about a user account:

- The username.
- The full name.
- The password.
- The roles associated with the account.
- Whether the account is enabled. If you disable an account while the user is currently logged in, the user is immediately prevented from taking any further actions.



**Note:** You can disable your own account. Once you disable it, however, you cannot reenable it yourself.

---

- Whether to force a password change at the next login.

You cannot change the user ID or type of authentication. (The user ID is displayed with other account details when you view an individual account as a user with the security role.)

To modify an existing user account (except its data access permissions and the allow namespace management property):

1. In the list of user accounts on the **Users** page, click on the username for the account you want to modify.
2. In the panel that opens, make the changes you want. For information on the fields and options in this panel, see ["Creating a user account"](#) above.



**Notes:**

- When changing the password for a user account, you can reuse the current password. You cannot do this when changing your own password on the **Change Password** page.
  - If you leave the **Password** field empty, the previously set password remains in effect.
- 

3. Click on the **Update Settings** button.

If you are modifying the user account you used to log into the Console and:

- You changed the roles associated with the user account, a message appears indicating that the page will be reloaded. Click on the **Close** button in the message window to reload the page.
- You selected the **Force change on next login** option, the Console displays the **Change Password** page. You need to change your password on this page in order to continue working in the Console.

## Deleting a user account

You can delete a user account at any time. If you delete an account while the user is currently logged in, the user is immediately prevented from taking any further action. After you delete the account, the user can no longer log in.



---

**Tip:** For a RADIUS-authenticated user, if the user account becomes invalid on the RADIUS server while the user is logged in, the user may still be able to take action in the current Console session for as long as ten minutes. To ensure that the user is immediately prevented from taking further action, delete the user in HCP before deleting the remote account.


---



You cannot recreate a deleted account. However, you can reuse the username from the deleted account to create a new account. The new account will have different user ID from the deleted account.

You cannot delete the account you used to log into the current Tenant Management Console session. Additionally, if no existing AD group has the security role, you cannot delete the last locally authenticated user account with the security role.

To delete a user account:

1. In the list of user accounts on the **Users** page, click on the delete control (  ) for the account you want to delete.
2. In response to the confirming message, click on the **Delete** button.

## Working with group accounts

To view, create, and manage HCP group accounts, you use the **Groups** page in the Tenant Management Console. This page is available only if the tenant supports AD authentication. For more information on AD authentication, see [“Active Directory authentication”](#) on page 72.

To display the **Groups** page:

1. In the top-level menu in the Tenant Management Console, mouse over **Security** to display a secondary menu.

2. In the secondary menu, click on **Groups**.



---

**Roles:** To:

- View the group account list, you need the monitor, administrator, or security role
  - View the full definitions of group accounts, you need the security role
  - View the allow namespace management property and data access permissions for group accounts, you need the monitor or administrator role
  - Create, associate roles with, and delete group accounts, you need the security role
  - Modify the allow namespace management property and data access permissions for group accounts, you need the administrator role
- 

## About the Groups page

The **Groups** page lets you create, modify, and delete HCP group accounts. It also lists the existing group accounts.



By default, the group account list includes all existing group accounts. The accounts are listed 20 at a time in ascending order by group name.

You can page through, sort, and filter the list of group accounts. The **Groups** page indicates which accounts are shown out of the total number of accounts in the current list.

To view additional information about an individual group account, click on the group name.

### Paging

You can change the number of group accounts shown at a time on the **Groups** page. To do this, in the **Items per page** field, select the number of group accounts you want. The options are 10, 20, and 50.

To page forward or backward through the group account list, click on the next (  ) or back (  ) control, respectively.

To jump to a specific page in the group account list:

1. In the **Page** field, type the page number you want.

2. Press Enter.


### Sorting


You can sort the group account list in ascending or descending order by group name. To change the sort order, click on the **Name** column heading. Each time you click on the column heading, the sort order switches between ascending and descending.

### Filtering

You can filter the group account list by group name. The filtered list includes only those group accounts with a name that begins with or is the same as a specified text string.

To filter the group account list:

1. In the entry field above the list, type the text string you want to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
2. Click on the find control (  ).

To redisplay the entire list of group accounts after filtering it, click on the clear filter control (  ).

## Creating group accounts

You create group accounts by first displaying a list of AD groups and then selecting the ones from which you want to create HCP group accounts. After selecting the groups you want, you select the roles you want to associate with those group accounts. If you have the administrator role, you can also associate data access permissions with the accounts.

You can create up to the maximum supported number of group accounts in a single operation (that is, 100).


In HCP, each AD group is identified by both the group name and the name of the AD domain in which the group is defined (for example, hcp-admin@ad.example.com). The HCP group account created from an AD group has the same name as the AD group, including the domain name. Internally, however, the HCP group account is associated with the security ID (SID) of the AD group.


You can create an HCP group account from any group defined in the AD forest that HCP uses for user authentication. The only exceptions are predefined groups such as Administrators that have the same SID in all domains.


You can use a single operation to both create new group accounts and change the roles and data access permissions associated with existing group accounts. In this case, all the accounts involved end up with the same roles and permissions.


To create group accounts:


1. On the **Groups** page in the Tenant Management Console, click on **Add Active Directory Groups**.

The **Find and Select Groups** section lists all the AD groups HCP knows about. Groups for which HCP group accounts already exist for the tenant are marked with a checkmark (  ).


2. Optionally, filter the list of AD groups:
  - a. In the **Find and Select Groups** field, type a text string to use as a filter for the list of AD groups from which you can create HCP group accounts. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
  - b. Click on the find control (  ).

To redisplay the entire list of AD groups after filtering it, click on the clear filter control (  ).

3. For each AD group from which you want to create an HCP group account, click on the add control (  ) to select the group. The group row turns green.

Also, for each AD group with an existing HCP group account for which you want to change the associated roles, click on the add control (  ) to select the group. The group row turns green.

To select all the groups in the list, click on the **Select All** button.

To deselect a selected group, click on the remove control (  ) for the group.

To deselect all the selected groups, click on the **Clear** button.

4. In the **Assign Roles to Selected Groups** section, select the roles you want to associate with all the new group accounts you're creating and all the existing group accounts for which you're changing the associated roles. You can select any number of roles, including none.

5. Optionally, if you have the administrator role, select the **Allow namespace management** option. (This option is selected automatically and cannot be deselected if the account being created has the administrator role.)
6. Optionally, if you have the administrator role, click on **Assign Namespace Permissions**. Then associate data access permissions with the group accounts, as described in ["Specifying permissions for any number of namespaces"](#) on page 87.
7. Click on the **Add Groups** button.

## Modifying a group account

You can change the roles associated with group accounts at any time. You can do this for an individual group account, as described below, or for multiple group accounts in a single operation, as described in ["Creating group accounts"](#) above.

To change the roles associated with an individual group account:

1. In the list of group accounts on the **Groups** page in the Tenant Management Console, click on the name of the group account you want to modify.
2. In the **Roles** section, select or deselect roles as applicable.
3. Click on the **Update Settings** button in the **Roles** section.

## Deleting a group account

You can delete a group account at any time. Deleting a group account has no effect on the corresponding group in AD.

When you delete a group account, AD users in the corresponding AD group immediately lose the roles and data access permissions granted by that group account.

If no existing HCP user account has the security role, you cannot delete the last group account with the security role.

When a group is deleted in AD, the corresponding HCP group account is not automatically deleted. However, the name of the group account changes to the SID of the deleted AD group. HCP group accounts that correspond to deleted AD groups serve no purpose and should be deleted.




---

**Note:** The Tenant Management Console may not immediately reflect the change to the HCP group account name.

---

To delete a group account:

1. In the list of group accounts on the **Groups** page in the Tenant Management Console, click on the delete control (  ) for the group account you want to delete.
2. In response to the confirming message, click on the **Delete** button.

## Changing the allow namespace management property for a user or group account

As a user with the administrator role, you can change the allow namespace management property for a user or group account. However, if the account has the administrator role, you cannot remove the allow namespace management property from the account.

To change the allow namespace management property for a user or group account:

1. In the list of user or group accounts on the **Users** or **Groups** page, as applicable, select the user account or group account you want.
2. Select or deselect the **Allow namespace management** option, as applicable.
3. Click on the **Update Settings** button.

## Changing the data access permissions for a user or group account

As a user with the administrator role, you can change the data access permissions associated with a user or group account. For a user account, you do this on the **Users** page in the Tenant Management Console. For a group account, you do this on the **Groups** page.

You can make these changes to data access permissions for a user or group account:

- Specify permissions for any number namespaces in a single operation
- Change the permissions for an individual namespace for which the user or group account already has one or more permissions
- Dissociate a namespace from the user or group account, thereby removing all permissions for that namespace

You can change the data access permissions associated with multiple group accounts in a single operation. For information on doing this, see [“Creating group accounts”](#) above.



---

**Note:** You cannot associate data access permissions with a RADIUS-authenticated user account.

---


## Specifying permissions for any number of namespaces


You associate data access permissions with a user or group account by first displaying a list of namespaces and then selecting the ones for which you want to specify data access permissions. After selecting the namespaces you want, you select the permissions you want the user or group account to have for those namespaces.


You can specify permissions for any number of namespaces in a single operation. If the user or group account already has permissions for any of the selected namespaces, the set of permissions you select replaces the set of permissions already associated with each of those namespaces.


To specify data access permissions for one or more namespaces:

1. In the list of user or group accounts on the **Users** or **Groups** page, as applicable, select the user account or group account you want.
2. Click on **Assign Namespace Permissions**.


The **Find and Select Namespaces** section lists all the namespaces owned by the tenant. Namespaces for which the user or group account already has any permissions are marked with a checkmark (  ).

3. Optionally, filter the list of namespaces by name:
  - a. In the **Find and Select Namespaces** field, type a text string to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
  - b. Click on the find control (  ).

To redisplay the entire list of namespaces after filtering it, click on the clear filter control (  ).

4. For each namespace for which you want to specify data access permissions, click on the add control (  ) to select the namespace. The namespace row turns green.

To select all the namespaces in the list, click on the **Select All** button.

To deselect a selected namespace, click on the remove control (  ) for the namespace.

To deselect all the namespaces after selecting all, click on the **Clear** button.

5. In the **Assign Data Access Permissions for Selected Namespaces** section, select the permissions you want the user or group account to have for the selected namespaces.

Selecting **Read** automatically selects **Browse**. Selecting **Search** automatically selects **Read** and **Browse**. Selecting **Purge** automatically selects **Delete**.

To select all the permissions, click on the **Select all** link.

To deselect all the selected permissions, click on the **Deselect all** link.

For descriptions of the data access permissions, see ["Data access permissions"](#) on page 69.

6. Click on the **Assign Namespaces** button.




## Changing the permissions for an individual namespace

To change the data access permissions associated with a user or group account for an individual namespace:

1. In the list of user or group accounts on the **Users** or **Groups** page, as applicable, click on the name of the user account or group account you want.

The panel that opens includes a list of the namespaces for which the user or group account already has data access permissions.

2. Optionally, filter the list of namespaces:
  - a. In the field above the **Name** column for the list of namespaces, select **Name** to filter the list by namespace name or **Tag** to filter the list by tag.
  - b. In the next field, type the text string you want to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
  - c. Click on the find control (  ).

To redisplay the entire list of namespaces after filtering it, click on the clear filter control (  ).

3. In the list of namespaces, click on the name of the namespace for which you want to change the data access permissions.
4. In the **Data Access Permissions** section, select or deselect permissions as needed.

Selecting **Read** automatically selects **Browse**. Selecting **Search** automatically selects **Read** and **Browse**. Selecting **Purge** automatically selects **Delete**.

To select all the permissions, click on the **Select all** link.

To deselect all the selected permissions, click on the **Deselect all** link.

Deselecting all permissions dissociates the namespace from the user or group account.

For descriptions of the data access permissions, see [“Data access permissions”](#) on page 69.


5. Click on the **Update Settings** button in the **Data Access Permissions** section.

## Dissociating a namespace from a user or group account


To dissociate a namespace from a user or group account, thereby removing all data access permissions for that namespace:

1. In the list of user or group accounts on the **Users** or **Groups** page, as applicable, click on the name of the user account or group account you want.

The panel that opens includes a list of the namespaces for which the user or group account already has data access permissions.

2. Optionally, filter the list of namespaces:
  - a. In the field above the **Name** column for the list of namespaces, select **Name** to filter the list by namespace name or **Tag** to filter the list by tag.
  - b. In the next field, type the text string you want to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
  - c. Click on the find control (  ).

To redisplay the entire list of namespaces after filtering it, click on the clear filter control (  ).

3. In the list of namespaces, click on the delete control (  ) for the namespace for which you want to remove all data access permissions.
4. In response to the confirming prompt, click on the **Delete** button.

## Changing user account and login settings

Several system settings affect user accounts and logins to the Tenant Management and Search Consoles. To view and change these settings, you use the **Console Security** page in the Tenant Management Console.

To display the **Console Security** page:

1. In the top-level menu in the Tenant Management Console, mouse over **Security** to display a secondary menu.

2. In the secondary menu, click on **Console Security**.




---

**Roles:** To view and change user account and login settings, you need the security role.

---

User account and login settings control:

- The minimum password length for locally authenticated HCP user accounts. Valid values are two through 64 characters. The default is six.
- The number of days after which locally authenticated users are automatically forced to change their passwords. Valid values are integers in the range zero through 999,999. The default is 180 days. A value of zero means users are never automatically forced to change their passwords.




---

**Note:** Password expiration affects the use only of the Tenant Management Console, Namespace Browser, and Search Console. Users with expired passwords can continue to use those passwords with the HCP management API, namespace access protocols, metadata query API, and HCP-DM. Password changes, however, affect all the HCP interfaces.

---

- The consecutive number of times a locally authenticated or RADIUS-authenticated user can enter an incorrect password before the user account is automatically disabled. Valid values are integers in the range zero through 999. The default is five. A value of zero means accounts are never disabled due to failed login attempts.

After a user account is automatically disabled, you need to reenable it manually to allow the user to log in again. For information on doing this, see [“Modifying a user account and its roles”](#) on page 79.

If the last locally authenticated user account with the security role is disabled due to failed login attempts and no group accounts have the security role, the user account is reenabled automatically after one hour.




---

**Note:** A user account with both roles and data access permissions can be disabled by consecutive attempts to use the HTTP protocol or Namespace Browser with an invalid password. A user account with only data access permissions is not disabled by these actions.

---

- The number of days an HCP user account can remain inactive before it's automatically disabled. Valid values are integers in the range zero through 999. The default is 180 days. A value of zero means accounts are never automatically disabled due to inactivity.

If no group accounts have the security role, the last locally authenticated user account with the security role is not automatically disabled due to inactivity.

- The number of minutes a Tenant Management Console, Search Console, or Namespace Browser session can be inactive before it times out. Valid values are integers in the range zero through 999. The default is ten minutes. A value of zero means sessions never time out due to inactivity.

When a session times out, the Console or Browser displays the **Idle Timeout** page. If you then select a page to display:

- If the user explicitly logged in, the Console or Browser login page appears.
- In the case of single sign-on, the Console or Browser displays the selected page in the Tenant Management Console or Namespace Browser or the **Simple Search** page in the Search Console.



---

**Tip:** If the tenant supports AD authentication and has no HCP user accounts, the recommended session timeout interval is eight hours.

---

- Message text to appear on the login page of the Tenant Management and Search Consoles. This text is optional. If specified, it can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.

The text you specify appears at the bottom of the login pages. You can use this text, for example, for messages such as "Authorized Users Only" or "Welcome to the Finance Department HCP Management Console."

To change one or more login settings, on the **Console Security** page:

- In the **Login Settings** section:
  1. Make the changes you want.
  2. Click on the **Update Settings**.

- In the **Login Message** section:
  1. Type the message you want.
  2. Click on the **Modify Login Message** button.



## Managing the current tenant

When you log into the Tenant Management Console, you do so for a particular tenant. You can then view all the available information about that tenant, change certain of its properties, and monitor its activity.

This chapter:

- Describes the tenant **Overview** page
- Contains instructions for configuring the current tenant
- Explains how to monitor tenant activity
- Explains how to monitor and manage tenant and namespace replication
- Describes chargeback reports and explains how to generate them

For an introduction to tenants, see [“Namespaces and tenants”](#) on page 3.

## About the tenant Overview page

When you log into the Tenant Management Console, the first page you see is the tenant **Overview** page. This page gives you a view of the tenant as a whole. It also shows the HCP system time.



---

**Roles:** To view the tenant **Overview** page, you need the monitor, administrator, security, or compliance role.

---

To return to the tenant **Overview** page from other Console pages, click on **Overview** in the top-level menu.

## Tenant statistics

The tenant **Overview** page shows three categories of statistics:

- **Storage** — This category shows:
  - **Quota** — The total number of bytes available to the tenant for allocation to its namespaces. This is the hard quota for the tenant.
  - **Used** — The total number of bytes currently occupied by stored data in all the namespaces owned by the tenant. This includes object data, metadata (except ACLs), and any redundant data required to satisfy the namespace DPLs.
  - **Available** — The number of bytes still available for storing data in the namespaces owned by the tenant.
- **Namespaces** — This category shows:
  - **Quota** — The number of namespaces reserved for the tenant out of the total number of namespaces the system can have. This is also the maximum number of namespaces the tenant can own at any given time. If the tenant doesn't have a quota, this field displays **No Quota**.
  - **Used** — The number of namespaces currently owned by the tenant.
  - **Available** — The number of additional namespaces the tenant can own if the tenant has a quota. If the tenant has no quota, this is the number of unallocated namespaces out of the total number of namespaces the system can have, minus the number of existing namespaces owned by tenants with no quota.



- **Objects Ingested** — The total number of objects currently stored in all the namespaces owned by the tenant. Multiple versions of an object are each counted as a separate object.
- **Objects Indexed** — The total number of indexed objects in all the namespaces owned by the tenant. This is the number of objects in the index maintained by the search facility that's currently selected for use with the Search Console.

This item appears only if the tenant has the search feature and a search facility is currently selected for use with the Search Console. In the case of the HDDS search facility, that facility must also be configured to show statistics.

- **Accounts** — This category shows:
  - The numbers of locally authenticated and RADIUS-authenticated user accounts defined for the tenant. This information is shown only if the tenant supports local or RADIUS authentication.
  - The number of group accounts defined for the tenant. This information is shown only if the tenant supports AD authentication and HCP support for AD is enabled at the system level.

## Major tenant events

The **Major Events** section on the tenant **Overview** page lists log messages about major events related to the tenant and its namespaces (for example, the tenant permission mask was changed or a namespace was created). The list includes all such messages that have occurred since the tenant was created.

The list of messages in the **Major Events** section is a subset of the messages in the event log for the tenant. You can view all the tenant-level messages in the tenant event log in the **All Events** panel on the **Tenant Events** page. For more information on the tenant **All Events** panel, see [“Viewing the complete tenant event log”](#) on page 109.

For a description of the information provided by each log message, see [“Understanding log messages”](#) on page 111. For information on the messages that can appear in the tenant log and how to respond to them, see [Appendix B, “Tenant log messages.”](#) on page 259.

By default, the messages in the **Major Events** section are listed ten at a time in reverse chronological order. For information on managing the message display, see [“Managing the message list”](#) on page 112.

If the **Overview** page shows alerts instead of log messages, click on the **Major Events** tab to display the log messages. For information on the alerts display, see ["Tenant alerts"](#) below.

## Tenant alerts

The **Alerts** section on the tenant **Overview** page shows alerts that indicate tenant-related conditions that may require human intervention (for example, the tenant is running low on unused space). This section is visible only if alerts currently exist for the tenant.

Each alert is represented by an icon accompanied by descriptive text. For information on the alerts that can appear in the **Alerts** section, see [Appendix A, "Tenant Management Console alerts,"](#) on page 253.

If the **Overview** page shows log messages instead of alerts, click on the **Alerts** tab to display the alerts. For information on the log message display, see ["Major tenant events"](#) above.



---

**Note:** If the tenant is read-only due to being a replication target or due to metadata unavailability, a notice of the situation appears at the top of every Tenant Management Console page. In this case, you cannot make any configuration changes to the tenant or to the namespaces it owns, nor can users and applications make any changes to namespace content. Additionally, in the case of metadata unavailability, statistics that describe namespace content may be inaccurate.

---

## Tenant features

The **Features** section on the tenant **Overview** page shows which of these features the tenant has:

- **Replication** — If this feature is present, the tenant is eligible for replication. Additionally, when you create a namespace, you have the option of selecting it to be replicated with the tenant. You can also select and deselect existing namespaces for replication.

If this feature is not present, the tenant cannot be replicated, and you cannot select or deselect namespaces to be replicated with it.

For information on replication, see ["Replication"](#) on page 32.

- **Retention Mode Selection** — If this feature is present, you can set the retention mode to either enterprise or compliance when you create a namespace. You can also change the retention mode of an existing namespace from enterprise to compliance, but you cannot do the reverse.

If this feature is not present, you can create namespaces only in enterprise mode and cannot change the retention mode of an existing namespace.

For information on enterprise and compliance modes, see [“Retention mode”](#) on page 16.

- **Search** — If this feature is present, you can create namespaces that support search. You can also enable and disable search for existing namespaces.

If this feature is not present, you cannot enable search for namespaces.

For information on search, see [Chapter 8, “Managing search and indexing.”](#) on page 203.

- **Service Plan Selection** — If this feature is present, you can associate service plans with namespaces.

If this feature is not present, you cannot associate service plans with namespaces.

For information service plans, see [“Service plans”](#) on page 45.

- **Versioning** — If this feature is present, you can create namespaces with versioning enabled. You can also enable and disable versioning for existing namespaces.

If this feature is not present, you cannot enable versioning for namespaces.

For information on versioning, see [“Versioning”](#) on page 23.

## Tenant contact information

You can view contact information for the current tenant from the tenant **Overview** page. To view this information, click on the **Contact Information** link.



---

**Roles:** To view the contact information for a tenant, you need the administrator role.

---

The contact information for a tenant is visible not only in the Tenant Management Console but also in the system-level administrative interface to the HCP system. HCP system administrators can use this information to notify you about systemwide events (such as a system shutdown for maintenance). Therefore, you should keep this information up to date.

For information on updating the tenant contact information, see [“Changing the tenant contact information”](#) on page 102.

## Tenant permission mask

The **Permissions** section on the tenant **Overview** page shows:

- The permissions included in the inherited permission mask, which is the systemwide permission mask. These permissions are indicated by gray dots.
- The permissions included in the tenant permission mask. These permissions are indicated by orange dots.
- The permissions included in the effective permission mask for the tenant. These permissions are indicated by checkmarks.

For an introduction to permission masks, see [“Data access permission masks”](#) on page 26. For information on modifying the tenant permission mask, see [“Changing the tenant permission mask”](#) on page 103.

## Tenant description

The **Description** section on the tenant **Overview** page shows the description of the tenant, if a description exists. This description is visible only in the Tenant Management Console. It is not visible to HCP system-level administrators who don't have administrative access to the tenant.

The tenant description appears below the tenant name on the login page for the Tenant Management Console.

For information on providing a description of the tenant, see [“Changing the tenant description”](#) on page 104.

## Configuring the tenant

You can change these properties of the current tenant:

- The tenant contact information
- The tenant permission mask
- The tenant description
- Whether HCP system-level users have administrative access to the tenant
- Which IP addresses have access to the Tenant Management Console for the tenant
- Whether programmatic access for tenant and namespace management is enabled for the tenant and, if so, which IP addresses have access to the tenant through the applicable APIs
- Which IP addresses have access to the Search Console for the tenant

You can also specify whether HCP should send tenant log messages to syslog servers, SNMP managers, and/or specified email addresses if these features are enabled at the HCP system level. For information on these options, see:

- [“Enabling syslog logging”](#) on page 113
- [“Enabling SNMP logging”](#) on page 113
- [“Configuring email notification”](#) on page 114

## Changing the tenant contact information

When creating a tenant, the HCP system administrator has the option of entering contact information for it. Once the tenant exists, both system-level administrators and tenant-level administrators can modify this information.



**Roles:** To view or modify the tenant contact information, you need the administrator role.

To provide contact information for the current tenant or to update the existing contact information:

1. In the top-level menu in the Tenant Management Console, click on **Overview**.
2. On the tenant **Overview** page, click on the **Contact Information** link.
3. In the **Contact Information** window, fill in the contact information. The table below describes the values you can specify. Except as indicated, all fields are optional.

Field	Description
<b>First Name</b>	First name of the tenant contact. First names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
<b>Last Name</b>	The last name of the tenant contact. Last names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
<b>Email</b>	An email address for the tenant contact. Email addresses cannot be more than 254 characters long.
<b>Confirm Email</b>	A repeat of the email address for the tenant contact. This field is required if you specify an email address in the <b>Email</b> field.
<b>Phone</b>	<p>A telephone number for the tenant contact. Do not include a telephone number extension. Instead, put the extension, if any, in the <b>Extension</b> field.</p> <p>Telephone numbers can contain only numbers, parentheses, hyphens (-), periods (.), plus signs (+), and spaces and can be up to 24 characters long (for example, (800) 123-4567).</p>
<b>Extension</b>	<p>A telephone number extension for the tenant contact.</p> <p>Telephone number extensions can contain only numbers and can be up to five characters long.</p>

*(Continued)*

Field	Description
<b>Address Line 1</b>	The first line of an address for the tenant contact. Address lines can be up to 100 characters long and can contain any valid UTF-8 characters, including white space.
<b>Address Line 2</b>	The second line of an address for the tenant contact.
<b>City</b>	The city for the tenant contact. City names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
<b>State/Province</b>	The state or province for the tenant contact. State and province names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.
<b>Postal Code</b>	The postal code for the tenant contact. Postal codes can be up to 64 characters long and can contain only alphanumeric characters and hyphens (-).
<b>Country</b>	The country for the tenant contact. Country names can be up to 64 characters long and can contain any valid UTF-8 characters, including white space.

4. Click on the **Update Contact Info** button.

For more information on tenant contact information, see [“Tenant contact information”](#) on page 100.

## Changing the tenant permission mask

When a tenant is created, its data access permission mask includes all permissions. You can change the permission mask for the current tenant at any time.




---

**Roles:** To change the tenant permission mask, you need the administrator role.

---

To change the tenant permission mask:

1. In the top-level menu in the Tenant Management Console, click on **Overview**.
2. On the tenant **Overview** page, click on the **edit** link for the **Permissions** section.

The Console displays a set of checkboxes for the possible permissions. The permissions that are currently in the tenant permission mask are selected.

3. Select or deselect permissions as needed to modify the permission mask.

Selecting **Purge** automatically selects **Delete**. Selecting **Search** automatically selects **Read**.

4. Click on the **Submit** button.

For an introduction to permission masks, see [“Data access permission masks”](#) on page 26. For more information on the tenant permission mask, see [“Tenant permission mask”](#) on page 100.

## Changing the tenant description

The tenant description is optional. You can enter a description or modify the existing description at any time.



---

**Roles:** To change the tenant description, you need the administrator role.

---

To change the tenant description:

1. In the top-level menu in the Tenant Management Console, click on **Overview**.
2. On the tenant **Overview** page, click on the **edit** link for the **Description** section.
3. In the edit area for the description, type the new description of the tenant. The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
4. Click on the **Submit** button.

For more information on the tenant description, see [“Tenant description”](#) on page 100.

## Enabling or disabling system-level administrative access

You can choose whether to grant HCP system-level users administrative access to the current tenant. By default, when a tenant is created, this access is not enabled. You can change this at any time.



---

**Roles:** To enable or disable system-level administrative access to the tenant, you need the administrator role.

---



To enable or disable system-level administrative access to the current tenant:

1. In the top-level menu in the Tenant Management Console, click on **Overview**.
2. On the tenant **Overview** page, do either of these:
  - To grant access, select the **Allow HCP system-level users to manage me and search across my space** option.
  - To deny access, deselect the **Allow HCP system-level users to manage me and search across my space** option.

For more information on system-level administrative access, see [“System-level administrative access”](#) on page 46.

## Controlling access to the Tenant Management Console

You can choose to allow access to the Tenant Management Console only from specific IP addresses. Similarly, you can choose to deny access to the Console from specific IP addresses.

You use the **Console Security** page in the Tenant Management Console to configure access to the Console. To display this page:

1. In the top-level menu in the Tenant Management Console, mouse over **Security** to display a secondary menu.
2. In the secondary menu, click on **Console Security**.




---

**Roles:** To view or modify the **Console Security** page, you need the security role.

---

To control access to the Tenant Management Console, on the **Console Security** page:

- Optionally, in the **Allow/Deny** section, specify IP addresses to be allowed or denied access to the Console. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.
- To specify how HCP should handle IP addresses that appear in both or neither of the **Allow** and **Deny** lists, select or deselect the **Allow request when same IP is used in both lists** option. Changes to this option take effect immediately.

For the effects of this option, see [“Allow and Deny list handling for HTTP, HS3, and WebDAV”](#) on page 183.

## Controlling access to HCP through the management API

For you to use the HCP management API with a tenant-level user account, the API must be enabled for both the HCP system and the tenant. Additionally, the API must be configured at the tenant level to allow access from your client IP address.

Enabling the management API also enables the use of the HS3 API to:

- Create namespaces
- List, view and modify the versioning status of, and delete namespaces you own

You use the **Management API** page in the Tenant Management Console to enable and configure the management API at the tenant level. To display this page:

1. In the top-level menu in the Tenant Management Console, mouse over **Security** to display a secondary menu.
2. In the secondary menu, click on **MAPI**.



---

**Roles:** To view and modify the HCP management API configuration, you need the security role.

---

To enable and configure the HCP management API, on the **Management API** page:

- To enable the management API, in the **Management API Settings** section:
  1. Select the **Enable the HCP management API** option.
  2. Click on the **Update Settings** button.
- Optionally, in the **Allow/Deny** section, specify IP addresses to be allowed or denied access to HCP through the management API. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.

- To specify how HCP should handle IP addresses that appear in both or neither of the **Allow** and **Deny** lists, select or deselect the **Allow request when same IP is used in both lists** option. Changes to this option take effect immediately.

For the effects of this option, see [“Allow and Deny list handling for HTTP, HS3, and WebDAV”](#) on page 183.

For a brief introduction to the management API, see [“HCP management API”](#) on page 49. For information on using the management API, see *HCP Management API Reference*.

## Controlling access to the Search Console

To use the HCP Search Console to search one or more namespaces, users log into the Search Console for the tenant that owns those namespaces. You can choose to allow access to the Search Console only from specific IP addresses. Similarly, you can choose to deny access to the Search Console from specific IP addresses.

You use the **Search Security** page in the Tenant Management Console to configure access to the Search Console. To display this page:

1. In the top-level menu in the Tenant Management Console, mouse over **Security** to display a secondary menu.
2. In the secondary menu, click on **Search Security**.




---

**Roles:** To view or modify the **Search Security** page, you need the security role.

---

To control access to the Search Console, on the **Search Security** page:

- Optionally, in the **Allow/Deny** section, specify IP addresses to be allowed or denied access to the Search Console. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.
- To specify how HCP should handle IP addresses that appear in both or neither of the **Allow** and **Deny** lists, select or deselect the **Allow request when same IP is used in both lists** option. Changes to this option take effect immediately.

For the effects of this option, see [“Allow and Deny list handling for HTTP, HS3, and WebDAV”](#) on page 183.

## Monitoring the tenant

While the tenant **Overview** page in the Tenant Management Console gives you a view of the tenant as a whole, the tenant log lets you monitor tenant and namespace activity on a more detailed level. The log records tenant and namespace events such as:

- Tenant Management Console logins
- Namespace creations
- Tenant and namespace configuration changes
- Creations, modifications, and deletions of retention classes
- Privileged delete operations
- Warnings about used storage approaching the hard quota

Each recorded entry about an event is called a **message**. The tenant log contains all the messages written to it since the tenant was created.

The Tenant Management Console provides several views of the log, as outlined in the table below.

View	Shows	More information
Tenant-level all events	All log messages recorded for the tenant and its namespaces	<a href="#">“Viewing the complete tenant event log”</a> below
Tenant-level major events	A subset of the log messages in the tenant-level all-events view	<a href="#">“Major tenant events”</a> on page 97
Tenant-level security events	Only log messages about attempts to log into the Tenant Management Console with an invalid username	<a href="#">“Viewing the tenant security log”</a> on page 110
Tenant-level compliance events	All log messages about events that require the compliance role across all the namespaces owned by the tenant	<a href="#">“Viewing the tenant compliance log”</a> on page 110
Namespace-level all events	All log messages for a given namespace	<a href="#">“Viewing the complete namespace event log”</a> on page 174
Namespace-level major events	A subset of the log messages in the namespace-level all-events view	<a href="#">“Major namespace events”</a> on page 142

*(Continued)*

View	Shows	More information
Namespace-level compliance events	All log messages about events that require the compliance role for a given namespace	<a href="#">"Viewing the namespace compliance log"</a> on page 175

In addition to these views of the log, HCP gives you the option of sending log messages to syslog servers, SNMP managers, and/or specified email addresses. For more information on this, see:

- ["Enabling syslog logging"](#) on page 113
- ["Enabling SNMP logging"](#) on page 113
- ["Configuring email notification"](#) on page 114

For information on the messages that can appear in the tenant log and how to respond to them, see [Appendix B, "Tenant log messages."](#) on page 259.

## Viewing the complete tenant event log

The **All Events** panel on the **Tenant Events** page lists all messages recorded for the tenant and its namespaces. By default, the panel displays ten messages at a time in reverse chronological order.




---

**Roles:** To view the tenant **All Events** panel, you need the monitor, administrator, security, or compliance role. However, only users with the compliance role can see messages about events that require the compliance role. Only users with the security role can see messages about attempts to log into the Tenant Management Console with an invalid username.

---

To display the **All Events** panel:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **Tenant Events**.
3. On the left side of the **Tenant Events** page, click on **All Events**.

For a description of the information provided by each log message, see ["Understanding log messages"](#) on page 111. For information on managing the message display, see ["Managing the message list"](#) on page 112.

## Viewing the tenant security log

The **Security Events** panel on the **Tenant Events** page lists all messages about attempts to log into the Tenant Management Console with an invalid username. By default, the panel displays ten messages at a time in reverse chronological order.



---

**Roles:** To view the tenant **Security Events** panel, you need the security role.

---

To display the **Security Events** panel:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **Tenant Events**.
3. On the left side of the **Tenant Events** page, click on **Security Events**.

For a description of the information provided by each log message, see ["Understanding log messages"](#) below. For information on managing the message display, see ["Managing the message list"](#) on page 112.

## Viewing the tenant compliance log

The **Compliance Events** panel on the **Tenant Events** page lists all messages about events that require the compliance role across all the namespaces owned by the tenant. This includes all retention class activity and privileged delete operations. By default, the panel displays ten messages at a time in reverse chronological order.



---

**Roles:** To view the tenant **Compliance Events** panel, you need the compliance role.

---

To display the **Compliance Events** panel:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **Tenant Events**.
3. On the left side of the **Tenant Events** page, click on **Compliance Events**.

For a description of the information provided by each log message, see [“Understanding log messages”](#) on page 111. For information on managing the message display, see [“Managing the message list”](#) on page 112.

For information on retention classes, see [Chapter 9, “Working with retention classes.”](#) on page 241. For information on privileged delete, see [Chapter 10, “Using privileged delete.”](#) on page 247.

## Understanding log messages

Each message displayed in a view of the tenant log includes this information about an event:

- The username of the event initiator:
  - For user-initiated events, this is the username currently associated with the user account used by the user who initiated the event. These considerations apply:
    - For an HCP user account, if the account has been deleted, the username is followed by the letter D in parentheses.
    - For an AD user account, if the account has been deleted or if HCP currently cannot contact AD, the username for the message is blank.
  - For system-initiated events, the username is **[internal]**.
  - For events initiated by HCP service or support personnel by means other than the Tenant Management Console, the username is **[service]**.

Additionally, when the tenant is being replicated, messages for events initiated by a user who accessed the Tenant Management Console directly from the HCP System Management Console have a username of **[remote admin]** in the log messages on systems to which the tenant is replicated.

- The severity of the event. Possible values are:
  - **Notice** — The event is normal and requires no special action. Events of this severity are informational only. Examples are:
    - Namespace created
    - Privileged delete requested

- **Warning** — The event is out of the ordinary and may require manual intervention. Examples are:
    - Namespace over soft quota
    - User account failed login
  - **Error** — The event is serious and most likely requires manual intervention. Examples are:
    - HCP found an irreparable object
    - Object did not replicate
- The date and time at which the event occurred, shown in the time zone of the HCP system.
  - A short description of the event.

To view more details about an event, click anywhere in the row containing the event message. To hide the details, click again in the row.

The details displayed for an event are:



- The user ID of the event initiator
- For user-initiated events, the port through which HCP received the event request
- For user initiated events, the IP address from which the event request was sent
- The message ID
- The full text of the event message

## Managing the message list

You can take the following actions in any of the views of the tenant log:

- To display details for all the listed events, click on the **expand all** link. To hide all details, click on the **collapse all** link.
- To view a different number of messages per page, select the number you want in the **Items per page** field.



- To page forward or backward, click on the next (  ) or back (  ) control, respectively.

## Enabling syslog logging

An HCP system can be configured to send system-level log messages to one or more specified syslog servers. You can choose to also send tenant log messages to those servers. The system-level configuration determines whether compliance and security messages are sent along with the other tenant log messages.

You use the **Syslog** page in the Tenant Management Console to enable or disable sending tenant log messages to the syslog servers. To display this page:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **Syslog**.




---

**Roles:** To view the **Syslog** page, you need the monitor or administrator role. To enable or disable syslog logging, you need the administrator role.

---

To enable or disable the logging of tenant log messages to syslog servers:

1. On the **Syslog** page, select (to enable) or deselect (to disable) the **Enable syslog logging** option.

If the HCP system is not configured for syslog logging, selecting this option has no effect.

2. Click on the **Update Settings** button.

## Enabling SNMP logging

An HCP system can be configured to send system-level log messages to one or more specified SNMP managers. You can choose to also send tenant log messages to those managers. The system-level configuration determines whether compliance and security messages are sent along with the other tenant log messages.

You use the **SNMP** page in the Tenant Management Console to enable or disable sending tenant log messages to the SNMP managers. To display this page:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **SNMP**.



---

**Roles:** To view the **SNMP** page, you need the monitor or administrator role. To enable or disable SNMP logging, you need the administrator role.

---

To enable or disable the logging of tenant log messages to SNMP managers:

1. On the **SNMP** page, select (to enable) or deselect (to disable) the **Enable SNMP logging** option.

If the HCP system is not configured for SNMP logging, selecting this option has no effect.

2. Click on the **Update Settings** button.

## Configuring email notification

HCP can be configured at the system level to support the use of email to notify recipients about messages added to the system-level log. If the HCP system supports email notification, you can configure HCP to send email about tenant log messages to recipients that you specify.

You can configure each email recipient to receive notification of only selected messages based on the message importance, severity, and type. Important messages are those that appear in the **Major Events** sections on the tenant **Overview** page and the **Overview** panel for each namespace in the Tenant Management Console. Message severity levels are notice, warning, and error. Message types are general, security, and compliance. In all cases, HCP makes a best effort to send the applicable email in a timely manner.

Recipients are added to the blind carbon copy (bcc) list for each email, so the recipients of an email are not visible to one another. The To list remains empty.

You can configure the content of the email that HCP sends. For example, you could choose to have HCP send the full text, severity, and date and time for each log message. Or, if you're concerned about exposing tenant and namespace information in what is by nature an insecure medium, you could format the email to say only that a log message was recorded.

HCP writes messages to the tenant log about email that the email server fails to accept. The messages about failed email are not sent to email recipients.

HCP replicates the tenant email configuration when replicating a tenant. However, the systems to which the tenant is replicated do not send email about log messages, so recipients don't receive duplicate notifications of events.

You use the **Email** page in the Tenant Management Console to enable and configure email notification. To display the **Email** page:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **Email**.




---

**Roles:** To view the **Email** page, you need the monitor or administrator role. To configure email notification, you need the administrator role.

---

## Enabling email notification

To have HCP send email about log messages, on the **Email** page:

1. Optionally, test whether email notification is supported. For instructions on this, see ["Testing email notification"](#) below.
2. Select the **Enable email notification** option.
3. Optionally, change the format of the email to be sent. For instructions on this, see ["Constructing the email message template"](#) on page 116.
4. Specify one or more recipients to receive email about log messages. For instructions on this, see ["Specifying email recipients"](#) on page 119.

## Testing email notification

HCP email notification works only if the HCP system has been configured to enable support for this feature. At any time, you can test the HCP system to determine whether it has been configured to support email notification.

Testing support for email notification causes HCP to send an email to an address that you specify. This email comes from the email address specified in the **From** field in the **Message Settings** section on the **Email** page. The email subject is "Test email from HCP."

To test whether email notification is supported, on the **Email** page:

1. Click on the **Test** button.
2. In the **Test Email Notification** window, type the email address to which you want HCP to send the test email.
3. Click on the **Send** button.

If support for email notification is not configured at the system level, the Tenant Management Console displays an error message. If the Console displays a success message but the email does not arrive, ensure that you've correctly specified the email address to which you want the email sent. If the email still doesn't arrive, contact your HCP system administrator for help.

## Constructing the email message template

The content of the email messages HCP sends is determined by the message template specified in the **Message Settings** section on the **Email** page. You can modify this template at any time. The **Message Preview** section shows a sample email that uses the current template.

The email template has three fields, each of which can be filled in with any combination of plain text and email template variables:

- The **From** field specifies the content of the email From line. This field must have a value. That value must have the form of a valid email address.

Some email servers require that the value in the From line be an email address that is already known to the server.

- The **Subject** field specifies the content of the email Subject line. This field must have a value.

For the email template subject, plain text can include spaces but not line breaks or tabs.

- The **Body** field specifies the body of the email. This field is optional.

For the email template body, plain text can include spaces and line breaks but not tabs. The character sequence consisting of a backslash (\) followed by a lowercase n creates a line break.

For a description of email template variables, see [“Email template variables”](#) below.

HCP comes with a default email template. At any time, you can change the email template back to the default. For instructions on this, see [“Restoring the default template”](#) on page 118.

To modify the template HCP uses for email notification about log messages, on the **Email** page:

1. In the **From**, **Subject**, and **Body** fields in the **Message Settings** section, specify the values that you want to use.
2. Optionally, click on the **Preview** button to preview the sample email with the specified format in the **Message Preview** field.
3. Click on the **Update Settings** button at the bottom of the page.

### Email template variables

The values you specify in the **From**, **Subject**, and **Body** fields in the email template can include variables that correspond to the information available for each log message (for example, the severity of the event that triggered the message or the short description of the event). When sending email, HCP replaces the variables in the email message with the applicable information.

To include a variable in the email template, you specify the variable name preceded by the dollar sign (\$). A dollar sign followed by anything other than a variable name is displayed as a dollar sign in the email HCP sends.

The table below lists the variables you can use in the email template.

Variable	Description
\$action	The action to take in response to the message
\$date	The date and time at which the event occurred (for example, Wed Feb 8 2012 3:15:57 PM EST)
\$fullText	The full text of the message
\$id	The message ID
\$location	The fully qualified name of the HCP system on which the event occurred (for example, hcp-ma.example.com)

*(Continued)*

Variable	Description
\$origin	For user-initiated events, the IP address from which the event request was sent and the port through which HCP received the event request, separated by a colon (for example, 192.168.152.181:8000)
\$reason	The reason why HCP issued the message
\$scope	Either Tenant or Namespace
\$severity	The severity of the event that triggered the message
\$shortText	A brief description of the event that triggered the message
\$type	The type of message (General, Security, or Compliance), preceded by Important and a comma if the message is important (for example, Important, Security)
\$user	The user ID and username of the event initiator (for example, 105ff38f-4770-4f98-b5b3-8371ab0af359 lgreen)

For more information on log messages, see [“Understanding log messages”](#) on page 111 and [Appendix B, “Tenant log messages.”](#) on page 259.

### Restoring the default template

The table below shows the format of the default email template.

Field	Default value
From	log@\$location
Subject	[\$severity] \$shortText
Body	<p>The following event occurred on \$date: \$fullText</p> <p>Reason: \$reason</p> <p>Action: \$action</p> <p>Details: User: \$user Origin: \$origin</p>

To change the email template back to the default, on the **Email** page:

1. Click on the **Reset** button.

2. Optionally, click on the **Preview** button to preview the sample email with the default format in the **Message Preview** field.
3. Click on the **Update Settings** button at the bottom of the page.

## Specifying email recipients

You use the **Recipients** section on the **Email** page to specify the email addresses to which HCP sends email about log messages. HCP sends email as blind carbon copies, so email recipients are not visible to one another.

Each row in the **Recipients** section contains one or more email addresses and indicates which messages are sent to those addresses. The section can have at most 25 rows.




Because each row in the **Recipients** section can contain multiple email addresses, you can specify a total of more than 25 addresses in this section. However, HCP sends each email only to an arbitrary 25 of the addresses that are supposed to receive the email. For example, if 34 email addresses are supposed to receive email about log messages that are important and have a severity level of error and a type of general, HCP sends such email only to 25 of those addresses.

You can add, modify, and delete rows in the **Recipients** section at any time.

### Understanding the recipients list

Each row in the **Recipients** section specifies:

- One or more email addresses.
- Whether to send email only about important log messages (**Major**) to the specified email addresses or to send email about all log messages (**All**).
- The severity of the log messages about which to send email:
  - **Notice** tells HCP to send email about log messages with a severity level of notice, warning, or error.
  - **Warning** tells HCP to send email about log messages with a severity level of warning or error.
  - **Error** tells HCP to send email only about log messages with a severity level of error.

- Whether to send email about general log messages (  ). General log messages are all messages that do not have a type of security or compliance.
- Whether to send email about log messages with a type of security (  ).
- Whether to send email about log messages with a type of compliance (  ).

Email recipients receive email only about log messages that have all the selected properties.

### **Adding, modifying, and deleting rows in the recipients list**


To add, modify, and/or delete rows in the recipients list, on the **Email** page:

1. Take one or more of these actions:

– To add a row:

1. Optionally, in the **Recipients** field, type a comma-separated list of one or more well-formed email addresses.
2. Click on **Add**.


A new row appears in the recipients list with importance set to **Major**, severity set to **Error**, and only general selected as the type. The row is highlighted in green.

To remove the new row, click on the delete control (  ) for the row.

– To modify a row:

- Optionally, in the **Address** field, type additional well-formed email addresses and/or modify or delete existing addresses. This field must contain at least one well-formed email address and no incorrectly formed addresses.
- Optionally, change the properties based on which HCP sends email to the specified addresses.

If you deselect all the types, no email is sent to the specified addresses.

– To delete a row, click on the delete control (  ) for the row.



The row turns red. To undo the deletion, click again on the delete control.

2. Click on the **Update Settings** button at the bottom of the page.

## Monitoring and managing replication

The **Replication** page in the Tenant Management Console shows information about replication of the current tenant when both of these conditions are true:

- The tenant is eligible for and currently selected for replication.
- The HCP system is configured to show this information.

If the tenant is eligible for but not currently selected for replication, the page shows a replication status of **Not Replicating**.

You can use the statistics and graphs on the **Replication** page to monitor replication progress. You can also use the page to select and deselect namespaces to be replicated along with the tenant.

To display the **Replication** page:

1. In the top-level menu in the Tenant Management Console, mouse over **Services** to display a secondary menu.
2. In the secondary menu, click on **Replication**.




---

**Roles:** To view the **Replication** page, you need the monitor or administrator role. To select and deselect namespaces for replication, you need the administrator role.

---

For an introduction to replication, see [“Replication”](#) on page 32.

## Tenant-level view of replication

At the tenant level, the **Replication** page shows:

- Only on an HCP system that’s sending data for the tenant to other systems, the approximate number of objects currently waiting to be replicated. This is the sum of the numbers of objects waiting to be replicated in each namespace selected for replication.

- Only on an HCP system that's sending data for the tenant to other systems, the approximate amount of data currently waiting to be replicated. This is the sum of the amounts of data waiting to be replicated in each namespace selected for replication.
- On an HCP system that's sending data for the tenant to other systems or receiving data for the tenant from other systems, the current rate of replication activity, expressed as operations per second and as bytes per second. An operation is the replication of a single item, such as the creation of a new object, a metadata change, or a namespace configuration change.

These rates are the sums of the corresponding rates for the namespaces owned by the tenant.

- A list of the namespaces selected for replication with the tenant. For each namespace, the list shows a progress bar that measures the up-to-date-as-of time for replication of that namespace, along with this time as a numeric value. The length of the progress bar represents 30 days, with the right end representing the current time.

The up-to-date-as-of time is the difference between:

- The time before which objects, metadata changes, and configuration changes are guaranteed to have been sent to other systems or received from other systems
- The current time



## Managing the namespace list

By default, the namespace list on the **Replication** page includes all the namespaces that are selected for replication. The namespaces are listed 20 at a time in ascending order by namespace name.

You can page through, sort, and filter the list of namespaces. The **Replication** page indicates which namespaces are shown out of the total number of namespaces in the current list.

### Paging

You can change the number of namespaces shown at a time on the **Replication** page. To do this, in the **Items per page** field, select the number of namespaces you want. The options are 10, 20, and 50.

To page forward or backward through the namespace list, click on the next (  ) or back (  ) control, respectively.

To jump to a specific page in the namespace list:

1. In the **Page** field, type the page number you want.
2. Press Enter.


### Sorting


You can sort the namespace list in ascending or descending order by namespace name. To sort the list, click on the **Name** column heading. Each time you click on the column heading, the sort order switches between ascending and descending.

### Filtering

You can filter the namespace list by namespace name or tag. The filtered list includes only those namespaces with a name or tag, as applicable, that begins with or is the same as a specified text string.

To filter the namespace list:

1. In the field above the **Name** column, select **Name** to filter by name or **Tag** to filter by tag.
2. In the next field, type the text string you want to use as a filter. This string can be up to 64 characters long, can contain any valid UTF-8 characters except commas (,), and is not case sensitive. White space is allowed.
3. Click on the find control (  ).

To redisplay the entire list of namespaces after filtering it, click on the clear filter control (  ).

## Namespace-level view of replication

To view more detailed information about the replication of an individual namespace listed on the **Replication** page, click on the namespace name. The panel that opens shows:

- The date and time before which objects, metadata changes, and configuration changes for the namespace are guaranteed to have been sent to other systems or received from other systems
- A graph of the history of the up-to-date-as-of time for replication of the namespace

- A graph of the history of the data transmission rate for replication of the namespace
- A graph of the history of the operation rate for replication of the namespace

On an HCP system that's sending data for the tenant to other systems, the panel also shows this information for the namespace:

**NOTE TO ME: One side for an active/active link is missing the objects and data pending information. See bug HCP-23877.**

- The approximate number of objects currently waiting to be replicated
- The approximate amount of data currently waiting to be replicated

### Up-to-date-as-of time

The **Up to date as of** section in the namespace replication panel contains a graph that shows the history of the up-to-date-as-of time for replication of the namespace. The section heading shows the current up-to-date-as-of time. If the graph is not currently visible, click on **Up to date as of** to display it.

The x-axis in this graph marks the passage of time. It shows 30 days (or fewer if replication has been occurring for less than 30 days). The y-axis marks the up-to-date-as-of time in days, hours, or minutes. As the up-to-date-as-of time varies, the measurement unit for the y-axis grows or shrinks as needed (for example, from days to hours to minutes). The lower the up-to-date-as-of time, the closer replication is to being synchronized with current namespace activity.

### Data transmission rate

The **Transfer Rate** section in the namespace replication panel contains a graph that shows the history of the rate of replication data transmissions for the namespace per second. The section heading shows the current data transmission rate. If the graph is not currently visible, click on **Transfer Rate** to display it.

The x-axis in this graph marks the passage of time. It shows 30 days (or fewer if replication or recovery has been occurring for less than 30 days). The y-axis marks the data transmission rate in KB, MB, or GB. As the transmission rate varies, the measurement unit for the y-axis grows or shrinks as needed (for example, from KB to MB to GB).

## Operation rate

The **Operations per Second** section in the namespace replication panel contains a graph that shows the history of the rate of replication operations for the namespace per second. The section heading shows the current operation rate. If the graph is not currently visible, click on **Operations per Second** to display it.

The x-axis in this graph marks the passage of time. It shows 30 days (or fewer if replication or recovery has been occurring for less than 30 days). The y-axis marks the operation rate in tens, hundreds, or thousands. As the operation rate varies, the measurement unit on the y-axis grows or shrinks as needed (for example, from tens to hundreds to thousands).

## Selecting or deselecting namespaces for replication

You can select or deselect namespaces to be replicated with the tenant at any time. If you deselect a namespace that was already being replicated, replication of that namespace stops. If you subsequently select that namespace again, replication of the namespace starts again from where it stopped.



**Note:** Depending on the current status of replication, if the tenant is being replicated, you may not be able to deselect namespaces.

---



**Important:** Depending on the configuration of the HCP systems in the replication topology, deselecting a namespace that has already been replicated may cause object data in that namespace to become inaccessible on one or more but not all of the systems in the topology.

---

To select or deselect namespaces for replication, on the **Replication** page:

1. Click on **Namespace Replication Selection**.

In the **Namespace Replication Selection** panel, the **Namespaces Selected for Replication** section lists the namespaces owned by the tenant that are currently selected for replication. The **Select Namespaces for Replication** section lists the namespaces owned by the tenant that are not currently selected for replication.

2. Take either or both of these actions:


– **To select namespaces for replication:**

1. Optionally, filter the list of namespaces in the **Select Namespaces for Replication** list by namespace name:

- a. In the **Select Namespaces for Replication** field, type a text string to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.

You cannot filter the namespace list while any of the namespaces in it are selected for replication.

- b. Click on the find control (  ).

To redisplay the entire list of unselected namespaces after filtering it, click on the clear filter control (  ).

2. For each listed namespace you want to select for replication, click in the namespace row.

The namespace is selected, and the namespace row change color.

To select all the namespaces in the list, click on the **Select All** button above the list.

To deselect a selected namespace, click in the namespace row.

To deselect all the selected namespaces, click on the **Clear** button.

– **To deselect HCP namespaces from replication:**

1. Optionally, filter the list of namespaces in the **Namespaces Selected for Replication** section, as described above.

2. For each listed namespace you want to deselect from replication, click in the namespace row.

The namespace is selected, and the namespace row changes color.

To select all the namespaces in the list, click on the **Select All** button above the list.

To deselect a selected namespace, click in the namespace row.

To deselect all the selected namespaces, click on the **Clear** button.



**Important:** Rows containing namespaces that have been deleted from HCP are highlighted in red and have a trash can icon (🗑️) on the right. HCP automatically removes each deleted namespace from the link after the deletion has been replicated.

Do not manually remove deleted namespaces from the link. If you do, the deletion will not be replicated.

3. Click on the **Update Selections** button.

If you deselected one or more namespaces and this action may result in inaccessible object data, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Update Selections** button.



**Tip:** You can also select or deselect a namespace for replication in the namespace **Replication** panel. For more information on doing this, see [“Changing replication options”](#) on page 168.

## Generating chargeback reports

You can generate chargeback reports from the Tenant Management Console. A **chargeback report** contains current and historical statistics about the tenant and its namespaces, broken out by hour.

Chargeback reports are a good source of information for namespace analysis, enabling you to adjust storage and bandwidth allocations based on usage patterns. These reports can also serve as input to billing systems that need to determine charges for capacity and bandwidth usage.

### About chargeback reports

A chargeback report contains statistics for each namespace owned by the current tenant. It also contains aggregated namespace statistics for the tenant. For example, the total number of reads for the tenant during a given reporting interval is the total number of successful read operations that occurred during that interval in each namespace owned by the tenant.

When generated from the Tenant Management Console, chargeback reports are in CSV format. Each line in a report contains the values for one namespace or for the tenant during one instance of the reporting interval.

The lines in a chargeback report are ordered alphabetically by namespace name. The lines for the tenant are at the end of the report. Multiple lines for a namespace or the tenant are ordered in ascending chronological order.

For information on how chargeback data is collected, see [“Chargeback statistics collection”](#) on page 129. For information on the contents of chargeback reports, see [“Chargeback report content”](#) on page 130.



---

**Roles:** To generate chargeback reports, you need the monitor or administrator role.

---

## Generating a chargeback report

You use the **Chargeback** page in the Tenant Management Console to generate chargeback reports. From this page, you can generate an hourly, daily, or monthly report:

- An **hourly report** includes statistics for the most recent full hour, plus the statistics accumulated so far for the current hour. For example, if you request the report at 2:30:15 p.m., it will contain one set of statistics for the period of time between 1:00:00 p.m. and 1:59:59 p.m. and another set of statistics for the period of time between 2:00:00 p.m. and 2:30:15 p.m.
- A **daily report** includes statistics for the most recent full day, plus the statistics accumulated so far for the current day. For example, if you request the report at 2:30:15 p.m. on October 7<sup>th</sup>, it will contain 24 sets of statistics for the period of time between 00:00:00 and 23:59:59 on October 6<sup>th</sup> and 15 sets of statistics for the period of time between 00:00:00 and 2:30:15 p.m. on October 7<sup>th</sup>.
- A **monthly report** includes statistics for the past 30 days, plus the statistics accumulated so far for the current day. For example, if you request the report at 2:30:15 p.m. on October 7<sup>th</sup>, it will contain 24 sets of statistics for each of the past 30 days and 15 sets of statistics for the period of time between 00:00:00 and 2:30:15 p.m. on October 7<sup>th</sup>.






---

**Note:** The statistics reported for the current hour may not reflect some reads and writes that have already occurred during the hour. After the hour is past, however, the statistics reported for it are complete.

---




---

**Tip:** You can use the HCP management API to generate chargeback reports that cover longer time periods and are in XML, JSON, or CSV format. This allows you to create applications that generate chargeback reports at regular intervals and feed those reports to a billing system. For information on using the management API to generate chargeback reports, see *HCP Management API Reference*.

---




---

**Roles:** To generate a chargeback report, you need the monitor or administrator role.

---

To generate a chargeback report:

1. In the top-level menu in the Tenant Management Console, mouse over **Monitoring** to display a secondary menu.
2. In the secondary menu, click on **Chargeback**.
3. On the **Chargeback** page, click on the **Hourly Chargeback Report**, **Daily Chargeback Report**, or **Monthly Chargeback Report** link, as applicable, and select the browser-specific option for downloading the report.

By default, the name of the downloaded report file is either `Hourly-Chargeback-Report.csv`, `Daily-Chargeback-Report.csv`, or `Monthly-Chargeback-Report.csv`, as applicable.

## Chargeback statistics collection

Chargeback statistics either reflect a point in time or are dynamic. Point-in-time statistics are measurements taken at the end of a reporting interval, such as the used storage capacity for a namespace at the end of an hour. Dynamic statistics are measurements, such as the number of reads or writes to a namespace, that are accumulated over time.

HCP accumulates dynamic statistics on an hourly basis, starting at the beginning of each hour. So, for example, one statistic might represent the number of successful writes to a namespace that occurred between 11:00:00 and 11:59:59. Another might represent the number of successful writes to the same namespace that occurred between 12:00:00 and 12:59:59.

## Chargeback report content

The first line of a chargeback report contains identifiers for the values in the subsequent lines. The table below describes each of these values and indicates whether it is point in time (P) or dynamic (D).

Identifier	Type	Value
systemName	N/A	The HCP domain name used for access to the content of namespaces owned by the identified tenant
tenantName	N/A	Either: <ul style="list-style-type: none"> <li>The name of the tenant that owns the namespace to which the set of statistics in the line applies</li> <li>The name of the tenant to which the set of statistics in the line applies</li> </ul>
namespaceName	N/A	The name of the namespace to which the set of statistics in the line applies.  In lines that contain tenant statistics, this field has no value.
startTime	N/A	The start time of the reporting interval for the set of statistics in the line, in this format:  <i>yyyy-MM-dd hh:mm:ss</i>  <i>hh</i> is hours on a 24-hour clock.  For example: 2010-10-07 14:00:00
endTime	N/A	The end time of the reporting interval for the set of statistics in the line, in the same format as is used for the startTime value.
objectCount	P	The number of objects in the identified namespace or in all the namespaces owned by the identified tenant.
ingestedVolume	P	The total size of the stored data and custom metadata, in bytes, before it was added to the identified namespace or to any of the namespaces owned by the identified tenant.
storageCapacityUsed	P	The total number of bytes occupied by stored data in the identified namespace or in any of the namespaces owned by the identified tenant. This includes object data, metadata, and any redundant data required to satisfy the applicable service plan.

*(Continued)*

Identifier	Type	Value
bytesIn	D	<p>The total number of bytes successfully written to the identified namespace or to any of the namespaces owned by the identified tenant during the reporting interval.</p> <p>If data was compressed before being transmitted, this is the number of bytes before compression.</p>
bytesOut	D	<p>The total number of bytes read from the identified namespace or from any of the namespaces owned by the identified tenant during the reporting interval.</p> <p>If data (including XML for directory listings) was compressed before being transmitted, this is the number of bytes before compression.</p>
reads	D	The total number of read operations performed in the identified namespace or in any of the namespaces owned by the identified tenant during the reporting interval.
writes	D	The total number of write operations successfully performed in the identified namespace or in any of the namespaces owned by the identified tenant during the reporting interval.
deletes	D	The total number of delete and purge operations successfully performed in the identified namespace or in any of the namespaces owned by the identified tenant during the reporting interval.
deleted	N/A	<p>One of:</p> <ul style="list-style-type: none"> <li>• <b>true</b> — For a namespace only, the namespace was deleted after the statistics in the set were collected.</li> <li>• <b>false</b> — The namespace or tenant currently exists.</li> <li>• <b>included</b> — For a tenant only, the statistics in the set include values for one or more namespaces that were subsequently deleted.</li> </ul>

*(Continued)*

Identifier	Type	Value
valid	N/A	<p>The status of the set of statistics in the line. Possible values are:</p> <ul style="list-style-type: none"><li>• <b>true</b> — HCP successfully collected all statistics in the set.</li><li>• <b>false</b> — The statistics in the set do not reflect all the activity that occurred during the reporting interval. This may be due, for example, to a network failure or to other hardware issues.</li></ul>

## Sample chargeback report

The next page shows an example of an hourly chargeback report, where the report was requested at 2:30:15 p.m. on October 7, 2012. It shows statistics for the Finance tenant, which owns the Accounts-Receiveable and Accounts-Payable namespaces. The report is shown as it would appear in a spreadsheet.

systemName	tenantName	namespaceName	startTime	endTime	objectCount	ingestedVolume	storageCapacityUsed	bytesIn	bytesOut	reads	writes	deletes	deleted	valid
hcp.example.com	Finance		2012-10-07 13:00:00	2012-10-07 13:59:59	1616	858071	884656	3399	1090	3	7	0	FALSE	TRUE
hcp.example.com	Finance		2012-10-07 14:00:00	2012-10-07 14:30:15	1623	860499	888832	3927	247	1	7	0	FALSE	TRUE
hcp.example.com	Finance	Accounts-Payable	2012-10-07 13:00:00	2012-10-07 13:59:59	376	162432	167936	494	529	2	2	0	FALSE	TRUE
hcp.example.com	Finance	Accounts-Payable	2012-10-07 14:00:00	2012-10-07 14:30:15	376	162432	167936	0	247	1	0	0	FALSE	TRUE
hcp.example.com	Finance	Accounts-Receivable	2012-10-07 13:00:00	2012-10-07 13:59:59	1240	692224	716720	2905	561	1	5	0	FALSE	TRUE
hcp.example.com	Finance	Accounts-Receivable	2012-10-07 14:00:00	2012-10-07 14:30:15	1247	705357	720896	3927	0	0	7	0	FALSE	TRUE



# Managing namespaces

When a tenant is first created, it has no namespaces. You use the Tenant Management Console to create them as needed.

After creating a namespace, you can view all the available information about it, change its properties, and monitor its activity. You can also delete namespaces that have no objects in them.

This chapter contains information on:

- Understanding the information displayed for namespaces
- Creating and deleting namespaces
- Configuring namespaces
- Changing the default settings for namespace creation
- Setting the maximum number of namespaces per user
- Monitoring namespace activity

## About the Namespaces page

To view, create, and manage namespaces, you use the **Namespaces** page in the Tenant Management Console. To display this page, in the top-level menu, click on **Namespaces**.

The **Create Namespace** bar on the **Namespaces** page shows the number of bytes of storage used in all the namespaces owned by the tenant, along with a graphical representation of the amount of storage used out of the hard quota for the tenant. It also shows the number of bytes of storage available for storing more objects in the namespaces owned by the tenant.

The **Namespaces** page also lists the namespaces owned by the current tenant. For information on this list, see [“Understanding the namespace list”](#) and [“Managing the namespace list”](#) below.



---

**Roles:** To view the **Namespaces** page, you need the monitor, administrator, or compliance role.

---

## Understanding the namespace list

The **Namespaces** page contains a list of the namespaces owned by the current tenant. For each namespace, the list shows:

- The namespace name.
- The number of objects currently in the namespace. Multiple versions of an object are each counted as a separate object.
- Icons for any current alerts that apply to the namespace. Alerts indicate conditions that may need your attention. To see the text that accompanies an alert icon, mouse over the icon.

For information about the alerts that can appear on the **Namespaces** page, see [“Namespaces page alerts”](#) on page 255.

- The number of bytes of storage used out of the hard quota for the namespace, along with a graphical representation of the amount of storage used.

To view additional information about an individual namespace, click on the namespace name.





## Managing the namespace list

By default, the namespace list on the **Namespaces** page includes all existing namespaces. The namespaces are listed 20 a time in ascending order by namespace name.

You can page through, sort, and filter the list of namespaces. The **Namespaces** page indicates which namespaces are shown out of the total number of namespaces in the current list.

### Paging

You can change the number of namespaces shown at a time on the **Namespaces** page. To do this, in the **Items per page** field, select the number of namespaces you want. The options are 10, 20, and 50.

To page forward or backward through the namespace list, click on the next (  ) or back (  ) control, respectively.

To jump to a specific page in the namespace list:

1. In the **Page** field, type the page number you want.
2. Press Enter.

### Sorting

You can sort the namespace list in ascending or descending order by namespace name or by hard quota. To sort the list, click on the column heading for the property you want to sort by. Each time you click on the column heading, the sort order switches between ascending and descending.

### Filtering

You can filter the namespace list by namespace name or tag. The filtered list includes only those namespaces with a name or tag, as applicable, that begins with a specified text string.


You can filter the namespace list by name or by tag by using the fields above the list. You can also filter the list by tag by using the tag control.

To filter the namespace list by name or tag using the filter fields:


1. In the field above the **Name** column, select **Name** to filter by name or **Tag** to filter by tag.

2. In the next field, type the text string you want to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.

3. Click on the find control (  ).

To redisplay the entire list of namespaces after filtering it, click on the clear filter control (  ).

To filter the namespace list by tag using the tag control:

1. Click on the tag control (  ) on the right above the namespace list.

The **Tags** window opens. This window lists all the tags currently associated with the existing namespaces owned by the current tenant. For each tag, the window shows the number of associated namespaces.

2. Click on the tenant-count icon (  ) for the tag you want.

The namespace list shows only the namespaces that have the selected tag, and the fields above the **Name** column show the filter criteria.

## About the namespace Overview panel

The namespace **Overview** panel shows the current status of any given namespace. To display this panel:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.

To return to the namespace **Overview** panel from other namespace panels, click on **Overview** in the row of tabs below the namespace name.



---

**Roles:** To view the namespace **Overview** panel, you need the monitor, administrator, or compliance role.

---

## Namespace URL

The top of the namespace **Overview** panel shows the URL for access to the namespace content through the HTTP protocol. If the HTTP protocol is enabled for the namespace, this URL is a link that opens the Namespace Browser for the namespace.

A namespace URL has this format:

`https://namespace-url-name.tenant-url-name.hcp-domain-name`

For example, the URL for access to the content of the Accounts-Receivable namespace owned by the Finance tenant in the HCP system named hcp-ma.example.com is:

`https://accounts-receivable.finance.hcp-ma.example.com`

If SSL security is not enabled for the HTTP protocol, the URL contains *http* instead of *https*.

For information on enabling or disabling HTTP and SSL security, see [“Configuring the HTTP, HS3, and WebDAV protocols”](#) on page 185. For information on the Namespace Browser, see *Using a Namespace*.



**Note:** The HCP domain name used for access to namespace content may not be the same as the domain name used for access to the tenant for management purposes. Be sure to give your namespace users the correct domain name.

Similarly, the IP addresses for the system may differ for these two purposes. For the IP addresses to use for namespace access, contact your HCP system administrator.

## Namespace owner

The top right corner of the namespace **Overview** panel shows the namespace owner if the namespace has an owner:

- If the owner user account is an HCP account, the panel shows the account username.

If the user account for the owner of a namespace is deleted, the namespace reverts to having no owner.

- If the owner user account is an AD account and:
  - HCP can retrieve the user account information from AD, the panel shows the account username along with the name of the AD domain in which the account is defined, in this format:  
*username@ad-domain-name*

- HCP cannot retrieve the user account information from AD, the panel shows the SID for the user account. This can happen if the AD user account was deleted or if HCP cannot communicate with AD.

In either case, the username or SID is a link that you can use to change the namespace owner. If the namespace has no owner, the top right corner of the panel shows the **Modify Owner** link, which you can use to assign an owner to the namespace.

For more information on namespace owners, see [“Namespace owner”](#) on page 18. For information on changing the owner of a namespace, see [“Changing the namespace owner”](#) on page 153.

## Objects section

The **Objects** section in the namespace **Overview** panel contains a graph showing the number of objects in the namespace during the past 30 days (or since the namespace was created if that was less than 30 days ago). Multiple versions of an object are each counted as a separate object.

While any of the search facilities is selected for use with the Search Console, the graph also shows the total number of indexed objects in the namespace during the past 30 days. For any point in time for which the indexed object count is shown, the count reflects the index maintained by the search facility that was selected for the Search Console at that time.



### Notes:

- If the HDDS search facility is selected for use with the Search Console, the graph shows the number of indexed objects only if that facility is configured to show statistics.
- For any period during which HCP cannot retrieve statistics from the HDDS server (for example, because the network connection is broken), the graph shows the number of indexed objects as zero.

---

The x-axis in the **Objects** graph marks the passage of time. The y-axis marks the number of objects. As the number of objects increases, the intervals on the y-axis get larger. The section heading indicates the current measurement unit (for example, thousands or millions).

The graph legend shows the most recent value for the number of objects stored (**Ingested object count**) and, if applicable, the number of indexed objects (**Indexed object count**).

Below the **Usage** section (see below), the **Overview** panel shows the date and time the **Objects** and **Usage** sections were last updated. To show the most current information in these sections, click on the **Refresh Now** link.

## Usage section

The **Usage** section in the namespace **Overview** panel contains a graph showing information about the namespace storage during the past 30 days (or since the namespace was created if that was less than 30 days ago).

The x-axis in the **Usage** graph marks the passage of time. The y-axis marks the amount of storage in gigabytes, terabytes, or petabytes, depending on the namespace size. The graph heading indicates the current measurement unit (gigabytes (GB), terabytes (TB), or petabytes (PB)).

The **Usage** graph shows:

- **Total storage capacity** — The hard quota for the namespace. For information on the hard quota, see [“Storage quotas”](#) on page 14.
- **Used storage capacity** — The total amount of storage space currently occupied by all data stored in the namespace, including object data, metadata (except ACLs), and any redundant data required to satisfy the namespace service plan. For information on DPL, see [“Data protection level”](#) on page 15.

**NOTE TO ME: Need to change cross-reference above to something about service plans.**

- **Ingested volume** — The total size of the stored data and custom metadata before it was added to the namespace. This value tells you how much data you have stored.

The graph legend shows the current value for each item.

Below the **Usage** section, the **Overview** panel shows the date and time the **Objects** and **Usage** sections were last updated. To show the most current information in these sections, click on the **Refresh Now** link.

## Major namespace events

The **Major Events** section in the namespace **Overview** panel lists log messages about major events related to the namespace (for example, the amount of storage used by the namespace exceeds the namespace soft quota). The list includes all such messages that have occurred since the namespace was created.

The list of messages in the **Major Events** section is a subset of the messages in the event log for the namespace. You can view all the messages in the namespace event log in the **All Events** panel for the namespace. For more information on the namespace **All Events** panel, see [“Viewing the complete namespace event log”](#) on page 174.

For a description of the information provided by each log message, see [“Understanding log messages”](#) on page 111. For information on the messages that can appear in the namespace log and how to respond to them, see [Appendix B, “Tenant log messages.”](#) on page 259.

By default, the messages in the **Major Events** section are listed ten at a time in reverse chronological order. For information on managing the message display, see [“Managing the message list”](#) on page 112.

If the **Overview** panel shows alerts instead of log messages, click on the **Major Events** tab to display the log messages. For information on the alerts display, see [“Namespace alerts”](#) below.

## Namespace alerts

The **Alerts** section in the namespace **Overview** panel shows alerts that indicate namespace-related conditions that may require human intervention (for example, the namespace is running low on unused space). This section is visible only if alerts currently exist for the namespace.

Each alert is represented by an icon accompanied by descriptive text. For information on the alerts that can appear in the **Alerts** section, see [“Namespace Overview panel alerts”](#) on page 256.

If the **Overview** panel shows log messages instead of alerts, click on the **Alerts** tab to display the alerts. For information on the log message display, see [“Major namespace events”](#) above.

## Namespace features

The **Overview** panel for a namespace shows which of these features are currently enabled for the namespace:

- **Replication** — If this feature is present, the namespace is included in replication of its owning tenant. If this feature is not present, the namespace is not included in replication of its owning tenant.

For information on this feature, see [“Replication”](#) on page 32. For information on selecting and deselecting namespaces for replication, see [“Selecting or deselecting namespaces for replication”](#) on page 125.

- **Search** — If this feature is present, search is currently enabled for the namespace. The namespace is searchable if its effective permission mask includes search. If this feature is not present, the namespace is not searchable.

For information on this feature, see [Chapter 8, “Managing search and indexing.”](#) on page 203. For information on the effective permission mask for a namespace, see [“Data access permission masks”](#) on page 26.

- **Versioning** — If this feature is present, users and applications can create multiple versions of objects in the namespace. If this feature is not present, the namespace does not support versioning.

For information on this feature, see [“Versioning”](#) on page 23. For information on enabling or disabling versioning for a namespace, see [“Configuring object versioning”](#) on page 164.

Additionally, the **Overview** panel shows:

- The **service plan** in effect for the namespace. This feature is present only if the tenant is allowed to associate service plans with namespaces. For information on service plans, see [“Service plans”](#) on page 45.
- The **retention mode** of the namespace. This is either enterprise or compliance. For information on enterprise and compliance modes, see [“Retention mode”](#) on page 16.
- The **cryptographic hash algorithm** for the namespace. For more information on this, see [“Cryptographic hash algorithm”](#) on page 16.

- The **DPL** for the namespace. For more information on this, see [“Data protection level”](#) on page 15.

## Namespace permission mask

The **Permissions** section in the namespace **Overview** panel shows:

- The permissions included in the inherited mask, which is the effective tenant permission mask. These permissions are indicated by gray dots.
- The permissions included in the namespace permission mask. These permissions are indicated by orange dots.
- The permissions included in effective permission mask for the namespace. These permissions are indicated by checkmarks.

For an introduction to permission masks, see [“Data access permission masks”](#) on page 26. For information on modifying the namespace permission mask, see [“Changing the namespace permission mask”](#) on page 151.

## Namespace description

The **Description** section in the namespace **Overview** panel shows the description of the namespace, if a description exists.

For information on providing or modifying the description of a namespace, see [“Changing the namespace description”](#) on page 152.

## Creating a namespace

You create namespaces in the Tenant Management Console. When you create a namespace, you set some of its properties. Other namespace properties have default settings that you can change only after the namespace has been created.

You can change most of the properties for existing namespaces. For information on changing namespace properties, see [“Configuring a namespace”](#) on page 149.



**Roles:** To create a namespace, you need the administrator role.

---



**Notes:**

- If the tenant supports Active Directory authentication, you can create a namespace only while HCP can communicate with AD.
- Under certain circumstances, the current state of replication for the tenant may prevent namespace creation.

To create a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. On the **Namespaces** page, click on **Create Namespace**.

The **Create Namespace** panel opens. Below the **Namespace Name** field, this panel shows the number of namespaces the tenant currently owns and the number of additional namespaces currently available for the tenant to create.

The default settings that appear in the **Create Namespace** panel are determined by the settings on the **Namespace Defaults** page. For information on changing these defaults, see ["Changing the default settings for namespace creation"](#) on page 171.

3. In the **Create Namespace** panel:
  - In the **Namespace Name** field, type a name for the namespace. HCP derives the hostname for the namespace from this name. The hostname is used in URLs for access to the namespace.

In English, the name you specify for a namespace must be from one through 63 characters long and can contain only alphanumeric characters and hyphens (-) but cannot start or end with a hyphen. In other languages, because the derived hostname cannot be more than 63 characters long, the name you specify may be limited to fewer than 63 characters.

Namespace names cannot contain special characters other than hyphens and are not case sensitive. White space is not allowed.

Namespace names cannot start with *xn--* (that is, the characters *x* and *n* followed by two hyphens).

The namespace name must be unique for the current tenant. Different tenants can have namespaces with the same name.

You can change the namespace name any time after you create the namespace, except while the CIFS or NFS protocol is enabled for the namespace. However, when you change the name, the URL for the namespace may change as well.

You can reuse namespace names that are not currently in use. So, for example, if you delete a namespace, you can give a new namespace the same name as the deleted namespace had.

- Optionally, specify an owner for the namespace:
  - If the owner has an HCP user account, select the **Local** option. Then type the username for the account in the **Namespace Owner** field.
  - If the owner has an AD user account, select the **Active Directory** option. Then, in the **Namespace Owner** field, type the account username along with the name of the AD domain in which the account is defined, in this format: *username@ad-domain-name*

For more information on namespace owners, see [“Namespace owner”](#) on page 18.

- Optionally, in the **Description** field, type a description of the namespace. The description can be up through 1,024 characters long and can contain any valid UTF-8 characters, including white space.
- In the **DPL** field, select the DPL for the namespace. The **Dynamic** option shows the current system-level DPL setting in parentheses.

For information on DPL, see [“Data protection level”](#) on page 15.



**Important:** Depending on the system configuration, setting the DPL to 1 (if allowed) without replicating the namespace can leave objects in the namespace unprotected. To find out whether objects are at risk with DPL 1, contact your HCP system administrator.

---

- In the **Hash Algorithm** field, select the cryptographic hash algorithm for the namespace.

For information on namespace hash algorithms, see [“Cryptographic hash algorithm”](#) on page 16.

- In the **Hard Quota** field, type the number of gigabytes or terabytes of storage to allocate to the namespace and select either **GB** or **TB** to indicate the measurement unit. Valid values are decimal numbers with up to two places after the period. The minimum is 1 (one) for GB and .01 for TB. The maximum value is the amount of space the tenant still has available to allocate to its namespaces.




---

**Tip:** To the right of the **Hard Quota** field, the panel shows the amount of space the tenant has already allocated to its namespaces and the amount of space it still has available to allocate.


---

For more information on hard quotas, see ["Storage quotas"](#) on page 14.

- In the **Soft Quota** field, type the percentage point at which you want HCP to notify the tenant that free storage space for the namespace is running low. Valid values are integers in the range ten through 95.

For more information on soft quotas, see ["Storage quotas"](#) on page 14.

- Optionally, associate tags with the namespace:
  1. Click on **Tags**.
  2. For each tag you want to associate with the namespace:
    - a. In the field in the **Tags** section, type a text string to be used as a tag. Tags must be from one through 64 characters long, can contain any valid UTF-8 characters except commas (,), and are not case sensitive. White space is allowed.
    - b. Click on **Add Tag**.

To remove a new tag, click on the delete control (  ) for the tag.

For more information on tags, see ["Namespace tags"](#) on page 19.

- Under **Replication**, select **On** to replicate the namespace along with the tenant or **Off** to exclude it from replication. The **Replication** option is present only if the tenant is allowed to create namespaces with replication enabled.



---

**Note:** Depending on current replication requirements, if the tenant is being replicated, this option may be selected automatically. In this case, you cannot deselect it.

---


For information on replication, see [“Replication”](#) on page 32.

- Under **Retention Mode**, select either **Enterprise** or **Compliance** to set the retention mode for the namespace. The **Retention Mode** option is present only if the tenant is allowed to create namespaces in compliance mode.

For information on retention mode, see [“Retention mode”](#) on page 16.

- Under **Search**, select **On** to enable search for the namespace or **Off** to disable search. The **Search** option is present only if the tenant is allowed to create namespaces with search enabled.

For information on enabling and disabling search, see [“Setting search and indexing options”](#) on page 238.

- In the **Service Plan** field, either type the name of an existing service plan or click on the arrow control (  ). If you click on the arrow control:

1. In the **Service Plans** window, select the service plan you want.
2. Click on the **Apply Service Plan** button.

The **Service Plan** field is present only if the tenant is allowed to associate service plans with namespaces.

For information on service plans, see [“Service plans”](#) on page 45.

- Under **Versioning**, select **On** to enable object versioning in the namespace or **Off** to disable it. The **Versioning** option is present only if the tenant is allowed to create namespaces with versioning enabled.

When you select **On**, you can also enable version pruning.

To enable version pruning, in the **Version Pruning** section, select the **Prune versions older than ... days** option and, in the option field, type the number of days old versions of objects must remain in the namespace before they are pruned. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means prune immediately.

4. Click on the **Create Namespace** button.

If setting the DPL to one can leave objects unprotected and the value in the **DPL** field is either **1** or **Dynamic (1)**, a confirming message appears. Also, if the version pruning option is unselected, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Create Namespace** button.

## Configuring a namespace

You can change these properties of a namespace:

- Name
- Permission mask
- Description
- Hard and soft quotas
- Owner
- Tags
- Default retention, shred, and index settings
- Minimum data access permissions
- Whether the use of ACLs is enabled and, if so, whether ACLs are enforced
- Retention-related settings

- Whether custom metadata XML checking is enabled
- Whether object versioning is enabled and, if so, the amount of time to keep old versions
- Compatibility settings
- Whether disposition is enabled
- Replication options
- Associated service plan
- DPL
- Retention mode (only from enterprise to compliance)

You can also:

- Enable and configure namespace access protocols for a namespace. For information on this, see [Chapter 7, “Configuring namespace access protocols.”](#) on page 179.
- Change search and indexing options for a namespace. For information on this, see [Chapter 8, “Managing search and indexing.”](#) on page 203.

## Changing the namespace name

You can change the name of a namespace any time, except while the HS3, CIFS, or NFS protocol is enabled for the namespace. However, when you change the name, the URL for the namespace may change as well.



---

**Note:** When you change the name of a namespace, AD single sign-on is automatically disabled for the HTTP protocol for that namespace. You can reenable it any time after the name change (as long as HCP can communicate with AD).

---



---

**Tip:** Be sure to notify the namespace users when you change the name of a namespace.

---



---

**Roles:** To change the name of a namespace, you need the administrator role.

---

To change the name of a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Settings**.
4. On the left side of the **Settings** panel, click on **Name**.
5. In the **New Namespace Name** field in the **Name** panel, type the new name for the namespace. For the rules for namespace names, see ["Creating a namespace"](#) on page 144.
6. Click on the **Update Name** button.

## Changing the namespace permission mask

When you create a namespace, its data access permission mask includes all permissions. Once the namespace exists, you can change its permission mask at any time.




---

**Roles:** To change a namespace permission mask, you need the administrator role.

---

To change the permission mask for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the namespace **Overview** panel, click on the **edit** link for the **Permissions** section.

The Console displays a set of checkboxes for the permissions. The permissions that are currently in the namespace permission mask are selected.

4. Select or deselect permissions as needed to modify the permission mask.

Selecting **Purge** automatically selects **Delete**. Selecting **Search** automatically selects **Read**.

5. Click on the **Submit** button.

For an introduction to permission masks, see [“Data access permission masks”](#) on page 26. For more information on the namespace permission mask, see [“Namespace permission mask”](#) on page 144.

## Changing the namespace description

The namespace description is optional. You can enter a description or modify the existing description at any time.



---

**Roles:** To change a namespace description, you need the administrator role.

---

To change the description of a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the namespace **Overview** panel, click on the **edit** link for the **Description** section.
4. In the edit area for the description, type the new description of the namespace. The description can be up through 1,024 characters long and can contain any valid UTF-8 characters, including white space.
5. Click on the **Submit** button.

## Changing namespace storage quotas

You can change both the hard quota and soft quota for a namespace at any time.




---

**Roles:** To change namespace quotas, you need the administrator role.

---



To change the hard and/or soft quota for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the modify quotas control (  ) for the namespace whose quotas you want to change.
3. In the **Modify Namespace Quota** window, do either or both of these:
  - In the **Hard Quota** field, type the number of gigabytes or terabytes of storage to allocate to the namespace and select either **GB** or **TB** to indicate the measurement unit. Valid values are integers greater than or equal to one.
  - In the **Soft Quota** field, type a new soft quota for the namespace. Valid values are integers in the range ten through 95.
4. Click on the **Update Quota** button.

For more information on hard and soft quotas, see [“Storage quotas”](#) on page 14.

## Changing the namespace owner

You can change or remove the owner of a namespace at any time.




---

**Roles:** To change or remove the owner of a namespace, you need the administrator role.

---

To change or remove the owner of a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In top right corner of the namespace **Overview** panel, click on the name of the current owner or the **Modify Owner** link, whichever is shown.

4. In the **Modify Namespace Owner** window, do either of these:
  - To specify a new namespace owner, do either of these:
    - If the owner has an HCP user account, select the **Local** option. Then type the username for the account in the **New Namespace Owner** field.
    - If the owner has an AD user account, select the **Active Directory** option. Then, in the **New Namespace Owner** field, type the account username along with the name of the AD domain in which the account is defined, in this format:  
*username@ad-domain-name*
  - To remove the current namespace owner, leave the **New Namespace Owner** field empty.
5. Click on the **Update Owner** button.

For more information on namespace ownership, see [“Namespace owner”](#) on page 18.

## Changing namespace tags

You can change the tags associated with a namespace at any time.



---

**Roles:** To view the tags associated with a namespace, you need the monitor or administrator role. To change the tags associated with a namespace, you need the administrator role.

---


To change the tags associated with a namespace:


1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Settings**.
4. On the left side of the **Settings** panel, click on **Tags**.

5. In the **Tags** panel:

- To associate a new tag with the namespace:
  1. In the field in the **Tags** section, type a text string to be used as a tag. Tags must be from one through 64 characters long, can contain any valid UTF-8 characters except commas (,), and are not case sensitive. White space is allowed.
  2. Click on **Add Tag**.

The row with the new tag is highlighted in green.

To remove a new tag, click on the delete control (  ) for the tag.

- To remove a tag from the namespace, click on the delete control (  ) for the tag.

The row with the tag turns red. To revert the removal before submitting your changes, click again on the delete control.

6. Click on the **Update Settings** button.

For more information on tags, see ["Namespace tags"](#) on page 19.

## Changing the default retention setting

When you create a namespace, its default retention setting is **Deletion Allowed**. Once the namespace exists, you can change this setting at any time. Valid values for this setting are:

- An offset from the time the object is created. You specify an offset as numbers of years, months, and/or days. For example, you could specify an offset of two years. Then, an object added to the namespace on March 10, 2011, at 9:45 a.m. would expire on March 10, 2013, at 9:45 a.m.
- A retention class. For information on retention classes, see ["About retention classes"](#) on page 242.
- One of these special values:
  - **Deletion Allowed** — The object can be deleted at any time.

- **Deletion Prohibited** — The object can never be deleted by means of a normal delete operation. If the namespace is in enterprise mode, however, the object can be deleted by means of a privileged delete operation.

Once an object has this retention setting, its retention setting cannot be changed.

- **Initial Unspecified** — The object cannot be deleted, but can have its retention setting changed to any other retention setting. This setting is useful for namespaces for which the only enabled namespace access protocol is SMTP.

- A fixed date in the future. In this case, the retention period for the object ends at the end of the specified day.



---

**Tip:** If you specify a fixed date, remember to change the default retention setting again before that date occurs. Otherwise, the default retention setting reverts to **Deletion Allowed** when the specified date arrives.

---




---

**Roles:** To view the default retention setting for a namespace, you need the monitor, administrator, or compliance role. To change the default retention setting for a namespace, you need the compliance role.

---

To change the default retention setting for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Policies**.
4. On the left side of the **Policies** panel, click on **Retention**.
5. In the **Default Retention Setting** section in **Retention** panel, do one of these:
  - To make the default retention setting an offset:
    1. In the **Retention Method** field, select **Offset**.
    2. Optionally, in the **Years** field, type a number of years. Valid values are integers in the range zero through 9,999.

3. Optionally, in the **Months** field, type a number of months. Possible values are integers in the range zero through 9,999.
  4. Optionally, in the **Days** field, type a number of days. Possible values are integers in the range zero through 9,999.
- To make the default retention setting a retention class:
    1. In the **Retention Method** field, select **Retention Class**.
    2. In the **Retention Class** field, select the retention class you want.
  - To make the default retention setting a special value:
    1. In the **Retention Method** field, select **Special Value**.
    2. In the **Special Value** field, select the special value you want.
  - To make the default retention setting a fixed date:
    1. In the **Retention Method** field, select **Fixed Date**.
    2. In the **Fixed Date** field, either type a date or click on the calendar control (  ) to select a date. If you type a date, use this format: *mm/dd/yyyy*. The date you type or select must be later than the current date.
- If you enter an invalid date using the correct date format, HCP tries to convert it to a real date. For example, if you enter 11/31/2015, HCP converts it to 12/01/2015.
6. Click on the **Update Settings** button in the **Default Retention Setting** section.

For more information on the default retention setting, see [“Default retention setting”](#) on page 19. For more information on retention settings in general, see *Using a Namespace*.

## Changing the default shred setting

When you create a namespace, its default shred setting is not to shred. Once the namespace exists, you can change this setting at any time.



**Note:** Once an object is marked for shredding, its shred setting cannot be changed.



---

**Roles:** To view the default shred setting for a namespace, you need the monitor, administrator, or compliance role. To change the default shred setting for a namespace, you need the compliance role.

---

To change the default shred setting for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Policies**.
4. On the left side of the **Policies** panel, click on **Shredding**.
5. In the **Shredding** panel, select (to shred) or deselect (not to shred) the **Shred on delete** option.
6. Click on the **Update Settings** button.

For more information on the default shred setting, see [“Default shred setting”](#) on page 20.

## Changing the default index setting

When you create a namespace, its default index setting is to index. Once the namespace exists, you can change this setting at any time.



---

**Roles:** To view the default index setting for a namespace, you need the monitor or administrator role. To change the default index setting for a namespace, you need the administrator role.

---

To change the default index setting for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Policies**.
4. On the left side of the **Policies** panel, click on **Indexing**.

5. In the **Indexing** panel, select (to index) or deselect (not to index) the **Index objects** option.
6. Click on the **Update Settings** button.

For more information on the default index setting, see [“Default index setting”](#) on page 20.

## Changing minimum data access permissions

When you create a namespace, the set of minimum data access permissions is empty both for all users (that is, authenticated users and users that access the namespace anonymously) and for authenticated users. Once the namespace exists, you can modify these sets at any time.




---

**Roles:** To view the minimum data access permissions for a namespace, you need the monitor or administrator role. To change the minimum data access permissions for a namespace, you need the administrator role.

---

To change the settings for minimum data access permissions for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Protocols**.
4. In the **Protocols** panel, click on **Minimum Data Access Permissions**.
5. In the **Minimum Data Access Permissions** panel, select or deselect permissions, as applicable, for all users (**Anonymous and Authenticated Access**) and for authenticated users (**Authenticated Access Only**).

Selecting **Read** automatically selects **Browse**. Selecting **Search** automatically selects **Read** and **Browse**. Selecting **Purge** automatically selects **Delete**.

By default, selecting a permission in the **Anonymous and Authenticated Access** row automatically selects the same permission in the **Authenticated Access Only** row and prevents the permission from being deselected in that row. For information on changing this behavior, see [step 6](#) below.

6. Optionally, to control the behavior of permission enforcement:

- a. Click on the **Advanced Configuration** link.
- b. Do either of these:
  - To ensure that authenticated users always have the minimum permissions for all users in addition to the minimum permissions for authenticated users regardless of whether the protocol they're using requires authentication, select the **Enforce anonymous permissions for authenticated users** option.

Selecting this option causes permissions in the **Authenticated Access Only** row to be selected automatically when you select the corresponding permissions in the **Anonymous and Authenticated Access** row.

- To allow unauthenticated users to have permissions that don't apply to authenticated users when those users are using a protocol that requires authentication, deselect the **Enforce anonymous permissions for authenticated users** option.

Deselecting this option allows you to select permissions in the two rows independently of each other.

7. Click on the **Update Settings** button.

For more information on minimum data access permissions, see [“Minimum data access permissions”](#) on page 28.

## Enabling the use of ACLs

When you create a namespace, the use of ACLs is disabled. Once the namespace exists, you can enable this feature. However, after enabling this feature, you cannot disable it.



---

**Roles:** To enable the use of ACLs for a namespace, you need the administrator role.

---

To enable the use of ACLs for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.



3. In the row of tabs below the namespace name, click on **Settings**.
4. On the left side of the **Settings** panel, click on **ACLs**.
5. In the **ACLs** panel, select the **Enable ACLs** option.
6. In response to the confirming prompt, click on the **Enable ACLs** button.

For more information on ACLs, see [“Access control lists”](#) on page 30.

## Changing the option to enforce ACLs

By default, when you enable the use of ACLs for a namespace, the option to enforce ACLs is enabled. You can enable or disable this option at any time while the use of ACLs is enabled.




---

**Roles:** To view or change the option to enforce ACLs for a namespace, you need the administrator role.

---

To change the option to enforce ACLs in a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Settings**.
4. On the left side of the **Settings** panel, click on **ACLs**.
5. In the **ACLs** panel, select or deselect the **Enforce ACLs** option to have HCP enforce or not enforce ACLs, respectively.
6. Click on the **Update Settings** button.

For more information on enforcing ACLs, see [“Access control lists”](#) on page 30.

## Changing retention-related settings

When you create a namespace:

- Changes to POSIX UIDs and GIDs, POSIX permissions, and object owners are not allowed for objects under retention

- Only add operations are allowed with custom metadata for objects under retention

Once the namespace exists, you can change these settings at any time.



---

**Roles:** To view retention-related settings for a namespace, you need the monitor, administrator, or compliance role. To change these settings for a namespace, you need the compliance role.

---

To change retention-related settings for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Policies**.
4. On the left side of the **Policies** panel, click on **Retention**.
5. In the **Retention Options** section in the **Retention** panel:
  - Optionally, select (to allow) or deselect (to disallow) the **Allow ownership and POSIX permission changes for objects under retention** option.
  - Optionally, change the custom metadata setting:
    - To allow the addition, deletion, and replacement of custom metadata for objects under retention, select the **Add, delete, and replace** option.
    - To allow only the addition of custom metadata for objects under retention, select the **Add only** option.
    - To disallow all custom metadata operations for objects under retention, select the **None** option.
6. Click on the **Update Settings** button in the **Retention Options** section.

For more information on:

- POSIX UIDs, GIDs, and permissions, see [“Default POSIX UID, GID, and permissions”](#) on page 21

- Ownership and permission changes for objects under retention, see [“Ownership and permission changes for objects under retention”](#) on page 22
- Custom metadata handling, see [“Custom metadata operations for objects under retention”](#) on page 22
- Ownership, permissions, and custom metadata in general, see *Using a Namespace*

## Enabling or disabling XML checking for custom metadata

When you create a namespace, custom metadata XML checking is enabled. You can change this setting at any time.




---

**Roles:** To view the custom metadata XML checking setting for a namespace, you need the monitor or administrator role. To change the custom metadata XML checking setting for a namespace, you need the administrator role.

---

To change the custom metadata XML checking setting for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Policies**.
4. On the left side of the **Policies** panel, click on **Metadata**.
5. In the **Metadata** panel, do one of these:
  - To enable custom metadata XML checking, select the **Check on ingestion that XML in custom metadata files is well-formed** option.
  - To disable custom metadata XML checking, deselect the **Check on ingestion that XML in custom metadata files is well-formed** option.
6. Click on the **Update Settings** button.

For more information on custom metadata XML checking, see [“XML checking for custom metadata”](#) on page 23.

## Configuring object versioning

When you create a namespace, you specify whether versioning is enabled or disabled for it. Once the namespace exists, you can change this setting at any time except while the WebDAV, CIFS, NFS, or SMTP protocol or appendable objects are enabled for the namespace.



---

**Note:** If a tenant is not allowed to create namespaces with versioning enabled, the versioning setting is not available for its namespaces.

---

When you enable versioning, you can also enable version pruning. If versioning has ever been enabled for a namespace, you can change the pruning settings for the namespace at any time regardless of whether versioning is currently enabled.



---

**Tip:** To immediately remove old versions of objects, set the number of days to keep them to zero.

---

HCP maintains a transaction log in which it records create, delete, purge, prune, and disposition operations performed on objects. HCP uses this log to respond to operation-based queries issued through the metadata query API.

For any given namespace, you can choose whether HCP should keep records of deletion operations (delete, purge, prune, and disposition) if the namespace has ever had versioning enabled. The amount of time for which HCP keeps deletion records is determined by the system configuration.



---

**Note:** In a namespace that was replicated but is not currently selected for replication, the following sequence of actions can cause objects that were deleted to reappear:

---

1. You deselect the option to keep records of deletion operations.
  2. You reselect the namespace for replication.
- 



---

**Roles:** To view the versioning settings for a namespace, you need the monitor or administrator role. To change the versioning settings for a namespace, you need the administrator role.

---

To configure object versioning:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Policies**.
4. On the left side of the **Policies** panel, click on **Versioning**.
5. In the **Versioning** panel:

- To enable or disable versioning, select or deselect the **Enable versioning** option, respectively.
- To enable or disable version pruning, select or deselect the **Prune versions older than ... days** option, respectively.

If you select this option, in the option field, type the number of days old versions of objects must remain in the namespace before they are pruned. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means prune immediately.

This option is available only if you select the **Enable versioning** option or if versioning has ever been enabled.

- To keep or not keep deletion records, select or deselect the **Keep deletion records for versioned objects** option, respectively.

6. Click on the **Update Settings** button.

If the version pruning option is unselected, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Update Settings** button.

For more information on object versioning, see ["Versioning"](#) on page 23.

## Changing compatibility settings

When you create a namespace:

- **atime** synchronization is disabled
- The ability to create appendable objects is disabled

You can change these settings at any time except that you cannot enable appendable objects while versioning is enabled.



---

**Roles:** To view the compatibility settings for a namespace, you need the monitor or administrator role. To change the compatibility settings, you need the administrator role.

---

To change the compatibility settings for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Settings**.
4. On the left side of the **Settings** panel, click on **Compatibility**.
5. In the **Compatibility** panel:
  - Optionally, select or deselect the **Synchronize POSIX atime values and object retention settings** option.
  - Optionally, select or deselect the **Allow appendable objects with CIFS and NFS** option.



---

**Note:** If you enable appendable objects, you also need to disable disposition. For information on doing this, see [“Changing disposition settings”](#) below.

---



---

**Note:** If you enable both **atime** synchronization and appendable objects, you also need to enable ownership and permission changes for objects under retention. For information on this option, see [“Changing retention-related settings”](#) on page 161.

---

6. Click on the **Update Settings** button.

For more information on compatibility settings, see [“Compatibility properties”](#) on page 24.

## Changing disposition settings

When you create a namespace, disposition is disabled for both objects with expired retention periods and objects flagged as replication collisions. Once the namespace exists, you can change these settings at any time.




---

**Roles:** To view the disposition settings for a namespace, you need the monitor, administrator, or compliance role. To change the disposition settings for a namespace, you need the compliance role.

---

To change the disposition settings for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Services**.
4. On the left side of the **Services** panel, click on **Disposition**.
5. In the **Disposition** panel:
  - To enable or disable disposition for objects with expired retention periods, select or deselect the **Automatically delete objects with expired retention periods** option, respectively.
  - To enable or disable disposition for objects flagged as replication collisions, select or deselect the **Automatically delete replication collision objects after ... days** option, respectively.

If you select this option, in the option field, type the number of days objects flagged as replication collisions must remain in the namespace before they are automatically deleted. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means delete immediately.

6. Click on the **Update Settings** button.

For more information on disposition, see [“Disposition”](#) on page 25.

## Changing replication options

When you create a namespace, the read-from-remote-system option and the option to service HTTP requests redirected from other HCP systems are both enabled, and the collision handling option is set to move objects. While the namespace is selected for replication, you can change these settings at any time. If the namespace is not selected for replication, these settings are hidden.

You may want to disable the option to service redirected requests if your applications cannot tolerate stale data or metadata. One way you could get stale data would be to request an object for which two versions exist but for which the current version hasn't been replicated yet. In this case, you would get the old version from another system in the replication topology.




---

**Tip:** You can select or deselect a namespace for replication in the same panel in which you set the read-from-remote-system and accept-requests options. For more information on namespace selection for replication, see [“Selecting or deselecting namespaces for replication”](#) on page 125.

---




---

**Roles:** To view the replication options for a namespace, you need the monitor or administrator role. To change the replication options for a namespace, you need the administrator role.

---

To change the replication options for a namespace (and at the same time select the namespace for replication if it's not already selected):

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Services**.
4. On the left side of the **Services** panel, click on **Replication**.
5. In the **Replication** panel, if the **Enable replication** option is not selected, select it.
6. Optionally:
  - To enable or disable the read-from-remote-system feature, select or deselect the **Enable read from remote system** option, respectively.



- To allow or disallow HTTP requests that target the namespace to be redirected from other systems, select or deselect the **Accept requests redirected from other systems in the replication topology** option, respectively.
- To change the collision handling option, click on **Collision Handling**. Then, in the **Collision Handling** section:
  - To have HCP move objects flagged as replication collisions to the .lost+found directory, select the **Move object to the .lost+found directory** option.
  - To have HCP rename objects flagged as replication collisions, select the **Rename object and store in the same location** option.

7. Click on the **Update Settings** button.

If you deselected the **Enable replication** option and this action may result in inaccessible object data, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Update Settings** button.

For more information on these options, see [“Replication”](#) on page 32.

## Changing the service plan

The service plan for a namespace is set when the namespace is created. You can change this setting at any time.




---

**Roles:** To view the service plan for a namespace, you need the monitor or administrator role. To change the service plan for a namespace, you need the administrator role.

---

To change the service plan for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Services**.
4. On the left side of the **Services** panel, click on **Service Plan**.

5. In the list of service plans, select the service plan you want.



---

**Note:** HCP system administrators can delete service plans regardless of whether they're associated with any namespaces. In this case, the service plan name remains associated with the applicable namespaces, but the service plan is not available to be selected for any namespaces. HCP uses the Default service plan for the namespaces associated with that service plan name.

---

In the list of service plans, a deleted service plan has no description.

---

6. Click on the **Update Settings** button.

For more information on service plans, see ["Service plans"](#) on page 45.

## Changing the retention mode

The retention mode of a namespace is either enterprise or compliance. You can change a namespace in enterprise mode to compliance mode, but you cannot do the reverse.



---

**Note:** If a tenant is not allowed to create namespaces in compliance mode, the retention mode setting is not available for its namespaces.

---

When you change the retention mode of a namespace from enterprise to compliance, you have no guarantee that objects that should have been retained were not already deleted.



---

**Important:** Changing the retention mode of a namespace may violate local regulations regarding data retention. Before taking this action, be sure you understand the implications.

---



---

**Roles:** To view the retention mode setting for a namespace, you need the monitor or administrator role. To change the retention mode of a namespace, you need the administrator role.

---

To change the retention mode of a namespace from enterprise to compliance:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.

3. In the row of tabs below the namespace name, click on **Settings**.
4. On the left side of the **Settings** panel, click on **Retention Mode**.
5. In the **Retention Mode** panel, select the **Compliance** option.
6. Click on the **Update Settings** button.

A confirming message appears.

7. In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Update Settings** button.

## Changing the default settings for namespace creation

When you open the **Create Namespace** panel to create a namespace, the panel shows default settings for many of the namespace properties. You can change the defaults for these settings at any time. Changing the default settings for namespace creation has no effect on the properties of existing namespaces.




---

**Roles:** To view the default settings for namespace creation, you need the monitor or administrator role. To change the default settings for namespace creation, you need the administrator role.

---

To change the default settings for namespace creation:

1. In the top-level menu in the Tenant Management Console, mouse over **Configuration** to display a secondary menu.
2. In the secondary menu, click on **Namespace Defaults**.
3. On the **Namespace Defaults** page:
  - Optionally, in the **Description** field, type a new description. By default, this field is blank.
  - Optionally, in the **DPL** field, select a different DPL. The default is Dynamic.
  - Optionally, in the **Hash Algorithm** field, select a different cryptographic hash algorithm. The default is SHA-256.

- Optionally, in the **Hard Quota** field, type a new number of gigabytes or terabytes of storage to allocate to the namespace and select either **GB** or **TB** to indicate the measurement unit. The default is 50 GB. The maximum value you can specify is equal to the hard quota for the tenant.
- Optionally, in the **Soft Quota** field, type a new percentage point at which you want HCP to notify the tenant that free storage space for the namespace is running low. The default is 85.
- Optionally, under **Replication**, change the selection. The default is **Off**.

The **Replication** option is present only if the tenant is allowed to create namespaces with replication enabled.

- Optionally, under **Retention Mode**, change the selection. The default is enterprise mode.

The **Retention Mode** option is present only if the tenant is allowed to create namespaces in compliance mode.

- Optionally, under **Search**, change the selection. The default is **Off**.

The **Search** option is present only if the tenant is allowed to create namespaces with search enabled.

- Optionally, in the **Service Plan** field, type the name of or select a different service plan. The default is the Default service plan.

The **Service Plan** field is present only if the tenant is allowed to associate service plans with namespaces.

- Optionally, under **Versioning**, change the selection. The default is **Off**.

The **Versioning** option and the pruning options below are present only if the tenant is allowed to create namespaces with versioning enabled.

- Optionally, change the selection for the **Prune versions older than ... days** option. By default, this option is unselected.

If you select this option, in the option field, type the number of days old versions of objects must remain in the namespace before they are pruned. Valid values are integers in the range zero through 36,500 (that is, 100 years). A value of zero means prune immediately.

For more information on these settings, see ["Creating a namespace"](#) on page 144.

4. Click on the **Update Settings** button.

If setting the DPL to one for a namespace can leave objects unprotected and the value in the **DPL** field is either **1** or **Dynamic (1)**, a confirming message appears. Also, if the version pruning option is unselected, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Update Settings** button.

For information on valid values for the default settings for namespace properties, see ["Creating a namespace"](#) on page 144.

## Setting the maximum number of namespaces per user

You can limit the number of namespaces that can be owned by a single user. By default, this limit is 100. You can change the limit at any time.

Changing this limit does not affect current namespace ownership. For example, if a user owns seven namespaces and you change the limit to five, that user still owns those seven namespaces even though that exceeds the new limit. However, the user cannot own any additional namespaces, and if namespaces are taken away from the user, the limit of five applies.




---

**Roles:** To view the limit on namespace ownership, you need the monitor or administrator role. To change the limit on namespace ownership, you need the administrator role.

---

To change the limit on namespace ownership:

1. In the top-level menu in the Tenant Management Console, mouse over **Configuration** to display a secondary menu.
2. In the secondary menu, click on **Miscellaneous**.

3. In the **Maximum Number of Namespaces per User** field, type the new limit. Valid values are integers in the range zero through 10,000.
4. Click on the **Update Settings** button.

## Monitoring a namespace

While the namespace **Overview** panel in the Tenant Management Console gives you a view of a namespace as a whole, these namespace views of the tenant log let you monitor namespace activity on a more detailed level:

- The namespace-level all-events view shows all log messages for a given namespace. For more information on this view, see [“Viewing the complete namespace event log”](#) below.
- The namespace-level compliance view shows all log messages about events that require the compliance role for a given namespace. For more information on this view, see [“Viewing the namespace compliance log”](#) on page 175.

Although unlikely, if HCP finds a broken object it cannot repair, it reports the event in the tenant log. In the Tenant Management Console, you can see a list of the irreparable objects in any given namespace. For more information on this, see [“Working with irreparable objects”](#) on page 175.

## Viewing the complete namespace event log

The namespace **All Events** panel lists all namespace-specific log messages. By default, the panel displays ten messages at a time in reverse chronological order.



---

**Roles:** To view the namespace **All Events** panel, you need the monitor, administrator, or compliance role. However, only users with the compliance role can see messages about events that require the compliance role.

---

To display the **All Events** panel for a given namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Monitoring**.

4. On the left side of the **Monitoring** panel, click on **All Events**.

For a description of the information provided by each log message, see [“Understanding log messages”](#) on page 111. For information on managing the message display, see [“Managing the message list”](#) on page 112.

## Viewing the namespace compliance log

The namespace **Compliance Events** panel lists all namespace-specific log messages about events that require the compliance role. This includes all retention class activity and privileged delete operations. By default, the panel displays ten messages at a time in reverse chronological order.




---

**Roles:** To view the namespace **Compliance** panel, you need the compliance role.

---

To display the **Compliance Events** panel:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Monitoring**.
4. On the left side of the **Monitoring** panel, click on **Compliance Events**.

For a description of the information provided by each log message, see [“Understanding log messages”](#) on page 111. For information on managing the message display, see [“Managing the message list”](#) on page 112.

For information on retention classes, see [Chapter 9, “Working with retention classes.”](#) on page 241. For information on privileged delete, see [Chapter 10, “Using privileged delete.”](#) on page 247.

## Working with irreparable objects

The HCP system keeps track of the irreparable objects it finds. You can view a list of these objects for any given namespace in the Tenant Management Console. To display this list:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.

2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Monitoring**.
4. On the left side of the **Monitoring** panel, click on **Irreparable Objects**.



---

**Roles:** To view the **Irreparable Objects** panel, you need the monitor or administrator role. To acknowledge irreparable objects, you need the administrator role.

---

For each object it lists, the **Irreparable Objects** panel shows the full path to the object (starting after `rest` or `data`) and the date and time at which HCP discovered that the object was irreparable. If the namespace has ever had versioning enabled, the list also shows the version ID of each object.

If HCP subsequently repairs a listed object, the object is removed from the list.

You can acknowledge irreparable objects in the **Irreparable Objects** panel. Acknowledging an object leaves a checkmark in the object row. You can use this option to distinguish objects you've already seen from objects that have recently become irreparable.

You can delete irreparable objects from a namespace through normal delete operations as long as the objects are not under retention (or by using privileged delete if the objects are under retention). When you delete an object, HCP removes it from the list of irreparable objects.





---

**Note:** Acknowledging that an object is irreparable does not delete the object from the namespace.

---

By default, the objects in the **Irreparable Objects** panel are listed ten at a time in reverse chronological order by discovery time:

- To view a different number of objects, select the number of objects you want in the **Items per page** field. The options are 10, 20, 50, and 100.
- To page forward or backward, click on the next (  ) or back (  ) control, respectively.



To acknowledge one or more objects in the list of irreparable objects:

1. In the **Irreparable Objects** panel, individually select the objects you want to acknowledge, or click on the **select all** link to select all the unacknowledged objects on the current page.

To undo all your selections, click on the **deselect all** link.

2. Click on the **Acknowledge Selected** button.




---

**Tip:** To acknowledge all objects, whether selected or not, on *all* pages in a single operation, click on the **Acknowledge All** button.

---

For information on deleting objects from namespaces, see *Using a Namespace*.

## Deleting a namespace

You can delete an empty namespace (that is, a namespace that doesn't contain any objects). You cannot delete namespaces that are not empty.

If a namespace is being replicated, you may not be able to delete it directly on all the HCP systems in the replication topology. However, if you delete it on one system, the deletion is replicated to the other systems.




---

**Important:** If the namespace you want to delete is being replicated, do *not* deselect it from replication before deleting it. If you deselect it first, the deletion is not replicated, and the namespace remains on the other systems to which it was replicated. Depending on the replication topology, you may not be able to delete the namespace on one or more of those other systems.

---




---

### Tips:

- To empty a namespace, use HCP Data Migrator. With HCP-DM, you can delete multiple directories and objects in a single job. For information on doing this, see *Using HCP Data Migrator*.
  - When a namespace is deleted, the chargeback statistics for it become unavailable. Therefore, before deleting a namespace for which you need these statistics, you should generate the applicable chargeback report. For information on generating chargeback reports, see [“Generating chargeback reports”](#) on page 127.
-




---

**Roles:** To delete a namespace, you need the administrator role.

---

To delete a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the delete control (  ) for the namespace you want to delete.
3. In response to the confirming message, click on the **Delete** button.

## Configuring namespace access protocols

HCP supports the HTTP, HS3, WebDAV, CIFS, NFS, and SMTP protocols for access to namespaces. You use these protocols to add, view, modify, and delete namespace content. Additionally, you can use HS3 to create, view or change the versioning status of, and delete namespaces.

Each protocol is configured separately for each namespace. Any given protocol can be enabled on some namespaces and disabled on others unless protocol optimization is configured for cloud only protocols.

This chapter provides instructions for enabling and configuring each of the supported protocols.

For information on using the HTTP, WebDAV, CIFS, and NFS protocols to access a namespace, see *Using a Namespace*. For information on using the HS3 protocol to access a namespace, see *Using the HCP HS3 API*.

## Namespace access protocol configuration

Users and applications have access to the content stored in namespaces through these industry-standard protocols: HTTP, HS3 (compatible with Amazon S3), WebDAV, CIFS, NFS, and SMTP. By default, when a namespace is created, the HTTP protocol is enabled and requires SSL security (HTTPS). The other protocols are initially disabled. For any namespace access to occur, at least one protocol must be enabled.



---

**Tip:** For enhanced security, keep unused namespace access protocols disabled.

---

When you enable a namespace access protocol, you also need to configure it. Each protocol, with the exception of HTTP, HS3, and WebDAV, has its own set of configuration options; HTTP, HS3, and WebDAV share a set of these options. Some configuration options are common to multiple protocols; others are protocol specific.



---

**Note:** If your system administrator has configured new namespaces to be optimized for cloud protocols only, you cannot configure new namespaces to use CIFS, NFS, WebDAV or SMTP without first disabling the optimize for cloud protocols only setting for that particular namespace. If you have already begun ingesting data in the namespace, you cannot disable cloud optimization. For more information about disabling the feature, see the [“Protocol optimizing a namespace”](#) on page 181.

---

To enable and configure the protocols for a namespace, you use the **Protocols** panel for that namespace in the Tenant Management Console. This panel has separate tabs for each protocol except HTTP, HS3, and WebDAV, which share a tab.

To display the **Protocols** panel for a namespace:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want to configure.
3. In the row of tabs below the namespace name, click on **Protocols**.



---

**Roles:** To view the **Protocols** panel, you need the monitor or administrator role. To enable, disable, and configure namespace access protocols, you need the administrator role.

---

## Protocol optimizing a namespace

After selecting an access protocol to use for a namespace, the tenant administrator should consider whether the namespace should be optimized for all access protocols or optimized for cloud access protocols only.

The optimized for all access protocols setting lets the namespace use any HCP supported access protocol to ingest objects. This mode is recommended if you intend to use non-cloud access protocols such as CIFS, NFS, WebDAV, SMTP.

Optimizing a namespace for cloud protocols increases the ingest rate of your namespace but also configures the namespace to ingest objects exclusively through cloud protocols (REST API, HS3, HSwift). This setting is recommended if you intend to only use cloud access protocols.




---

**Note:** Once a namespace is optimized for cloud protocols and has begun ingesting objects, it cannot revert back to using all access protocols.

---

To optimize namespace access protocols, make sure that the HCP system is *not* upgrading by checking the System Management Console **Overview** page for warnings and follow these steps:

1. In the Tenant Management Console, click on the **Namespaces** section on the top-level navigation menu.
2. On the **Namespace** page, click on the **Namespace** you want to optimize.
3. In the namespace, click on the **Settings** tab.
4. In the namespace left-hand navigation bar, click on the **Optimization** button.
5. On the **Optimization** page, select **Optimized for all protocols** or **Optimized for cloud protocols only**.




---

**Note:** Usually the **Optimized for all protocols** setting is the default setting on this page. However, the **Optimize for cloud protocols only** setting might already be enabled by your system administrator. If the namespace has not begun ingesting data, you may deactivate optimized for cloud by selecting **Optimized for all protocols**.

---

6. Click on the **Update Settings** button.

7. In the **Confirm: Optimize Namespace for Cloud Protocols Only** window, type *YES* in the text field.
8. Click on the **Update** button.

## IP addresses for namespace access

For each namespace access protocol, you have the option of allowing access only from specific IP addresses. For all but NFS, you can also deny access to the namespace from specific IP addresses.



---

**Tip:** For enhanced security, restrict access to namespaces to as few IP addresses as possible.

---


The Tenant Management Console panels for the namespace access protocols each contain an **Allow** list and, except for the **NFS** panel, a **Deny** list. Each list has an associated field in which you type entries for it.

## Adding and removing entries in Allow and Deny lists

To add an entry to an **Allow** or **Deny** list:

1. In the field above the list, type the entry you want. For a description of valid entries, see [“Valid Allow and Deny list entries”](#) below.
2. Click on **Add**.

To remove entries from the **Allow** or **Deny** list:

- To remove a single entry, click on the delete control (  ) for that entry.
- To remove all entries, click on **Delete All**.

Changes you make to either list of IP addresses take effect immediately.

## Valid Allow and Deny list entries

Each entry in an **Allow** or **Deny** list can be one of:

- An IP address
- A comma-separated list of IP addresses

- A range of IP addresses specified as *ip-address/subnet-mask* (for example, 192.168.100.197/255.255.255.0) or in CIDR format (for example, 192.168.100.0/24)

The CIDR entry that matches all IP addresses is 0.0.0.0/0.

## Allow and Deny list handling

IP addresses can be included in neither, one, or both of the **Allow** and **Deny** lists for HTTP, HS3, WebDAV, CIFS, and SMTP. They can be included or not included in the **Allow** list for the NFS protocol. The way HCP handles allowed and denied IP addresses differs depending on the protocol.

### Allow and Deny list handling for HTTP, HS3, and WebDAV

For HTTP and WebDAV, you can choose how HCP handles **Allow** and **Deny** list entries by selecting or deselecting the **Allow request when same IP is used in both lists** option in the **HTTP(S)** panel. The table below describes the effects of selecting or deselecting this option. Either action takes effect immediately.

List entries	Allow Requests When Same IP Is Used in Both Lists	
	Selected	Not selected
<b>Allow</b> list: empty <b>Deny</b> list: empty	All IP addresses can access the namespace through HTTP, HS3, and WebDAV.	No IP addresses can access the namespace through HTTP, HS3, or WebDAV.
<b>Allow</b> list: at least one entry <b>Deny</b> list: empty	All IP addresses can access the namespace through HTTP, HS3, and WebDAV.	Only IP addresses in the <b>Allow</b> list can access the namespace through HTTP and WebDAV.
<b>Allow</b> list: empty <b>Deny</b> list: at least one entry	All IP addresses not in the <b>Deny</b> list can access the namespace through HTTP, HS3, and WebDAV. IP addresses in the <b>Deny</b> list cannot.	No IP addresses can access the namespace through HTTP, HS3, or WebDAV.
<b>Allow</b> list: at least one entry <b>Deny</b> list: at least one entry	IP addresses appearing in both or neither of the lists can access the namespace through HTTP, HS3, and WebDAV.	Only IP addresses appearing in the <b>Allow</b> list and not in the <b>Deny</b> list can access the namespace through HTTP, HS3, or WebDAV.

**Allow and Deny list handling for CIFS**

For CIFS, HCP handles **Allow** and **Deny** list entries as described in the table below.

List entries	Effect
<b>Allow</b> list: empty <b>Deny</b> list: empty	All IP addresses can access the namespace through the CIFS protocol.
<b>Allow</b> list: at least one entry <b>Deny</b> list: empty	Only IP addresses in the <b>Allow</b> list can access the namespace through the CIFS protocol.
<b>Allow</b> list: empty <b>Deny</b> list: at least one entry	All IP addresses that are not in the <b>Deny</b> list can access the namespace through the CIFS protocol. IP addresses in the <b>Deny</b> list cannot.
<b>Allow</b> list: at least one entry <b>Deny</b> list: at least one entry	All IP addresses appearing in the <b>Allow</b> list and only those addresses can access the namespace through the CIFS protocol, regardless of whether those addresses also appear in the <b>Deny</b> list.

**Allow list handling for NFS**

For NFS, if the **Allow** list in the **NFS** panel includes one or more IP addresses, those addresses have access to the namespace through NFS and all others don't. If the list is empty, all IP addresses can access the namespace through NFS.

**Allow and Deny list handling for SMTP**

For SMTP, HCP handles **Allow** and **Deny** list entries as described in the table below.

List entries	Effect
<b>Allow</b> list: empty <b>Deny</b> list: empty	All IP addresses can access the namespace through the SMTP protocol.
<b>Allow</b> list: at least one entry <b>Deny</b> list: empty	Only IP addresses in the <b>Allow</b> list can access the namespace through the SMTP protocol.
<b>Allow</b> list: empty <b>Deny</b> list: at least one entry	No IP addresses can access the namespace through the SMTP protocol.
<b>Allow</b> list: at least one entry <b>Deny</b> list: at least one entry	Only IP addresses appearing in the <b>Allow</b> list and not in the <b>Deny</b> list can access the namespace through the SMTP protocol.

**User authentication options**

The HTTP, HS3, and CIFS protocols have the option to either require user authentication or support both authenticated and unauthenticated (anonymous) access. If a protocol requires authentication, users must



present valid credentials in order to use the protocol. If a protocol supports both types of access, users can present credentials but are not required to.

With the HTTP, HS3, or CIFS protocol configured to support both authenticated and anonymous access:

- If a user presents credentials, HCP tries to authenticate the user. If the credentials are valid, HCP continues processing the request. If the credentials are invalid, HCP rejects the request.
- With HTTP and CIFS, if a user does not present credentials, HCP continues processing the request.
- With HS3, if a user presents the clear-text username `all_users`, HCP continues processing the request. If the user does not present either credentials or `all_users`, HCP rejects the request.

For more information on authentication, see [“User authentication”](#) on page 70.

## Configuring the HTTP, HS3, and WebDAV protocols

With the HTTP and HS3 protocols, users and applications can add, view, and delete objects and modify object metadata through a RESTful API. With the WebDAV protocol, users and applications can perform these activities through familiar directory structures.

### HTTP, HS3, and WebDAV protocol configuration

You use the **HTTP(S)** panel to enable and configure the HTTP, HS3, and WebDAV protocols for a namespace. To display this panel, on the left side of the **Protocols** panel, click on **HTTP(S)**.

Although you use a single panel to enable these protocols, you enable or disable them independently of each other.

The top of the **HTTP(S)** panel shows the URL for access to the namespace through the HTTP protocol. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with *https*. If only the HTTP port is open, the URL starts with *http*.

The **HTTP(S)** panel lets you:

- Enable the HTTP protocol.
- Enable the HS3 protocol.
- Enable the WebDAV protocol.
- Specify whether the HTTP, HS3, and WebDAV protocols require the use of SSL security.
- Specify whether the HTTP and HS3 protocols require user authentication for access to the namespace.
- If the tenant supports user authentication with Active Directory, specify whether HCP supports AD single sign-on for HTTP and HS3 access to the namespace. This affects the Namespace Browser, HCP Search Console, and other HTTP applications that support Integrated Windows authentication.
- Specify whether the WebDAV protocol requires basic authentication for access to the namespace.
- If WebDAV basic authentication is enabled, specify the username and password against which HCP authenticates WebDAV access to the namespace.

The username and password you specify for WebDAV basic authentication has no relationship to HCP or AD user accounts.



---

**Tip:** Be sure to give WebDAV users the specified username and password.

---

- Specify whether WebDAV dead properties can be stored as custom metadata. If they can be, they are stored in the annotation named default.
- Specify the client IP addresses that have access to the namespace through HTTP and WebDAV.

By default, when a namespace is first created, the HTTP protocol is enabled with authentication and SSL security required.

## Considerations for the HS3 API

These considerations apply to the HS3 API:

- You can enable the HS3 protocol for a namespace only while ACLs are enabled for the namespace. For information on enabling ACLs, see [“Enabling the use of ACLs”](#) on page 160.
- For users and applications to be able to perform any operations with the HS3 API, the HCP management API must be enabled for the tenant. For information on enabling the management API, see [“Controlling access to HCP through the management API”](#) on page 106.
- For a user or application to be able to create and manage namespaces with the HS3 API, the applicable user or group account must have the allow namespace management property enabled. For information on the allow namespace management property, see [Chapter 4, “Managing accounts.”](#) on page 61.

This additional consideration applies when you enable the HS3 API for a namespace that was created in an HCP release earlier than 6.0.

After being upgraded from a release earlier than 6.0, HCP generates ETags for objects that were stored before the upgrade. HCP generally does this over time. However, in response to an HS3 request to retrieve an object that does not yet have an ETag, HCP immediately generates the ETag before returning the object. This can be time consuming for large objects, with the result that HCP may be slow to respond to the first **GET** request for such an object. If you are concerned about this issue, please contact your HCP system administrator before enabling HS3 for the namespace.



**Note:** An ETag is an identifier for the content of the object. As of release 6.0, HCP generates ETags for objects at the time they are stored.

---

## Enabling HTTP, HS3, and WebDAV access to a namespace

The **HTTP(S)** panel has two sections for enabling and configuring the HTTP, HS3, and WebDAV protocols.

### Settings section

To enable the HTTP, HS3, and WebDAV protocols, in the **Settings** section:

1. Do either or both of these:
  - To open the HTTPS port for HTTP, HS3, and WebDAV access to the namespace with SSL security, select the **Enable HTTPS** option.
  - To open the HTTP port for HTTP, HS3, and WebDAV access to the namespace without SSL security, select the **Enable HTTP** option.

These two options are independent of each other. If you select only the **Enable HTTPS** option, data sent through the HTTP, HS3, and WebDAV protocols is always secure. If you select both options, users and applications can send both secure and unsecure data through the HTTP, HS3, and WebDAV protocols.



---

**Note:** To enable access to the namespace through the HTTP, HS3, or WebDAV protocol, you also need to select the **Enable REST API**, **Enable HS3 API**, or **Enable WebDAV API** option, respectively. Opening the HTTPS and HTTP ports does by itself enable these protocols.

---

2. To enable the HTTP protocol:
  - a. Select the **Enable REST API** option. This option is available only if the **Enable HTTP** or **Enable HTTPS** option is already selected.

Above the **Enable REST API** option, the panel shows the URL for access to the namespace through the HTTP protocol. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with *https*. If only the HTTP port is open, the URL starts with *http*.
  - b. To specify HTTP authentication requirements, below **Enable REST API** option, the select either the **Authenticated access only** option or the **Anonymous and authenticated access** option. For information on these options, see [“User authentication options”](#) on page 184.

- c. Optionally, select or deselect the **Enable Active Directory single sign-on** option to allow or disallow, respectively, single sign-on to the namespace with Active Directory authentication. This option appears only if the tenant supports AD for user authentication.

**Notes:**

- The option to enable AD single sign-on for HTTP is synchronized with the same option for HS3. Enabling or disabling either enables or disables the other, respectively.
  - To help ensure that AD single sign-on is available for those namespaces that need it, enable it only for those namespaces.
  - After this option is disabled, you can reenable it only while HCP can communicate with AD.
- 

## 3. To enable the HS3 protocol:

- a. Select the **Enable HS3 API** option. This option is available only if the **Enable HTTP** or **Enable HTTPS** option is already selected.

Above the **Enable HS3 API** option, the panel shows the URL for access to the namespace through the HS3 protocol. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with *https*. If only the HTTP port is open, the URL starts with *http*.

- b. To specify HS3 authentication requirements, below **Enable HS3 API** option, select either the **Authenticated access only** option or the **Anonymous and authenticated access** option. For information on these options, see ["User authentication options"](#) on page 184.
- c. Optionally, select or deselect the **Enable Active Directory single sign-on** option to allow or disallow, respectively, single sign-on to the namespace with Active Directory authentication. This option appears only if the tenant supports AD for user authentication.

## 4. To enable the WebDAV protocol:

- a. Select the **Enable WebDAV API** option. This option is available only if the **Enable HTTP** or **Enable HTTPS** option is already selected.

Above the **Enable WebDAV API** option, the panel shows the URL for access to the namespace through the WebDAV protocol. If the HTTPS port is open or if neither the HTTPS or HTTP port is open, this URL starts with *https*. If only the HTTP port is open, the URL starts with *http*.

- b. Optionally, to enable WebDAV basic authentication, select the **Enable WebDAV basic authentication** option. Then:
- In the **Username** field, type the username to use for basic authentication. Usernames must be from one through 64 characters long and can contain any valid UTF-8 characters but cannot start with an opening square bracket ([). White space is allowed.

Usernames are not case sensitive.

- In the **Password** field, type the password to use for basic authentication. Passwords can be up to 64 characters long, are case sensitive, and can contain any valid UTF-8 characters, including white space. The minimum password length is the same as the minimum password length for HCP user accounts, which is configurable.

To be valid, a password must include at least one character from two of these three groups: alphabetic, numeric, and other.

If you're modifying settings in the **HTTP(S)** panel and you leave the **Password** field empty, the previously set password remains in effect.

- In the **Confirm Password** field, type the password again.



---

**Tip:** Be sure to tell WebDAV users the username and password you specify.

---

- c. Optionally, to enable WebDAV users to store dead properties as custom metadata, select the **Use custom metadata to store WebDAV properties** option.

5. Click on the **Update Settings** button.

If you selected **Enable HTTP** and also selected **Enable REST API**, **Enable HS3 API**, or **Enable WebDAV API**, a confirming message appears. In response to this message, click on the **Update Settings** button.

**Allow/Deny section**

To set the IP addresses to be allowed or denied access to the namespace through HTTP, HS3, and WebDAV:

- Optionally, in the **Allow/Deny** section, specify IP addresses to be allowed or denied access to the namespace through HTTP, HS3, and WebDAV. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.
- To specify how HCP should handle IP addresses that appear in both or neither of the **Allow** and **Deny** lists, select or deselect the **Allow request when same IP is used in both lists** option. Changes to this option take effect immediately.

For the effects of this option, see [“Allow and Deny list handling for HTTP, HS3, and WebDAV”](#) on page 183.

## Configuring the CIFS protocol

With the CIFS protocol, users and applications can add, view, and delete objects and modify object metadata through familiar directory structures.

### CIFS protocol configuration

You use the **CIFS** panel to enable and configure the CIFS protocol for a namespace. To display this panel, on the left side of the **Protocols** panel, click on **CIFS**.

The top of the **CIFS** panel shows the string to use to identify the namespace when mapping it to a network drive or adding it as a network place on a CIFS client.

The **CIFS** panel lets you:

- Enable the CIFS protocol.

- Specify whether the CIFS protocol requires user authentication for access to the namespace. HCP uses Active Directory to authenticate CIFS users. This authentication is possible only if the tenant is configured to support AD authentication.



---

**Note:** If the HCP system does not support Active Directory and CIFS is enabled for the namespace, the namespace is exposed as a share in the Windows workgroup specified in the HCP system configuration. However, if the CIFS protocol is configured to require authentication, the namespace cannot be accessed through the workgroup.

---

- Specify the client IP addresses that have access to the namespace through CIFS.
- Change CIFS case sensitivity (see [“CIFS case sensitivity”](#) below).

When you reconfigure the CIFS protocol while it's already enabled, the changes you make don't affect current CIFS mounts of the namespace. To force the changes to take effect, you can do either of these:

- Disable and then reenabale the protocol. This causes all CIFS clients to lose their connections to the namespace. When they reconnect, the changes will be in effect.
- Direct all clients with current CIFS mounts to disconnect from the namespace and then to either reboot or wait five minutes for cached connections to be released before reconnecting.

For information on using the CIFS protocol for namespace access, see *Using a Namespace*.

## CIFS case sensitivity

The Windows operating system is case preserving but not case sensitive. The HCP CIFS implementation, by default, is both case preserving and case sensitive. One result of this discrepancy is that Windows applications that do not observe differences in case may not be able to access HCP objects by name.



For example, suppose a Windows application adds a file named `File.txt` to the namespace by using the CIFS protocol. CIFS preserves case, so the namespace then contains an object named `File.txt`. Now suppose the application tries to retrieve that object using the name `file.txt`. CIFS is case sensitive, so it passes the request to HCP with only the name `file.txt`. It doesn't include any case variations on the name, such as `File.TXT`, `FILE.txt`, or `File.txt`. As a result, HCP cannot find the object.

If you have Windows applications that ignore case, you may want HCP to ignore case as well. You can change the CIFS protocol configuration in either of two ways to meet this need:

- **Make CIFS case forcing** — With this behavior, CIFS changes names to all upper- or lowercase in the requests it passes to HCP. To Windows applications, then, HCP appears to be case-insensitive. An application that stores `File.txt` and then retrieves `File.TXT` will get the right object back.

The drawback to this method is that applications using other namespace access protocols must accommodate this behavior. For example, suppose CIFS changes names to all uppercase. If an application using the CIFS protocol stores an object named `File.txt`, applications using the case-sensitive HTTP, WebDAV, and NFS protocols need to retrieve the object as `FILE.TXT`.

- **Make CIFS case insensitive** — With this behavior, CIFS preserves case as objects are stored in the namespace but passes through every case variation possible when applications make other requests for objects.

For example, suppose an application using the CIFS protocol requests an object named `FILE.txt`. CIFS passes the request through with the names `File.txt`, `FILE.txt`, `file.TXT`, and so on. HCP then returns the first object it finds with a name that matches any of these.

The major drawback to this method is that performance is slowed by the need to check for matches to multiple case variations. A second drawback is that if the namespace contains multiple objects with names that vary only in case, HCP may return the wrong object.

If you make CIFS both case forcing and case insensitive, it is case forcing when storing objects and case insensitive on requests for existing objects.

For more information on CIFS case sensitivity, see *Case Sensitivity versus Case Preservation in CIFS Server (Samba)* at [http://www.manualshark.org/manualshark/files/28/pdf\\_27202.pdf](http://www.manualshark.org/manualshark/files/28/pdf_27202.pdf).

## Enabling CIFS access to a namespace

The **CIFS** panel has three sections for enabling and configuring the CIFS protocol.

### Settings section

To enable the CIFS protocol, in the **Settings** section:

1. Select the **Enable CIFS** option.
2. To specify CIFS authentication requirements, select either the **Authenticated access only** option or the **Anonymous and authenticated access** option. For information on these options, see [“User authentication options”](#) on page 184.
3. Click on the **Update Settings** button in the **Settings** section.

### Allow/Deny section

Optionally, in the **Allow/Deny** section, specify IP addresses to be allowed or denied access to the namespace through CIFS. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.

For information on how HCP handles IP addresses that appear in both or neither of the **Allow** and **Deny** lists, see [“Allow and Deny list handling for CIFS”](#) on page 184.

### Case Sensitivity section

To change CIFS case sensitivity:

1. Click on **Case Sensitivity**.
2. In the **Case Sensitivity** section:
  - To make the CIFS protocol case insensitive, deselect the **Make CIFS case sensitive** option.



---

**Note:** Disabling CIFS case sensitivity has a significant negative impact on performance.

---

- To make the CIFS protocol case forcing, select **Make CIFS case forcing**. Then select either **Lowercase** or **Uppercase** to force object names to be lowercase or uppercase, respectively.
3. Click on the **Update Settings** button in the **Case Sensitivity** section.

For more information on making the CIFS protocol case insensitive or case forcing, see [“CIFS case sensitivity”](#) on page 192.

## Configuring the NFS protocol

With the NFS protocol, users and applications can add, view, and delete objects and modify object metadata through familiar directory structures.

### NFS protocol configuration

You use the **NFS** panel to enable and configure the NFS protocol for a namespace. To display this panel, on the left side of the **Protocols** panel, click on **NFS**.

The top of the **NFS** panel shows the string to use to identify the namespace when mounting it on an NFS client.

The **NFS** panel lets you:

- Enable the NFS protocol.
- Specify default values for POSIX UIDs and GIDs. For information on these defaults, see [“Default POSIX UID, GID, and permissions”](#) on page 21.
- Specify the client IP addresses that have access to the namespace through NFS.

For information on using the NFS protocol to access stored data, see *Using a Namespace*.

### Enabling NFS access to a namespace

The **NFS** panel has two sections for enabling and configuring the NFS protocol.

#### Settings section

To enable the NFS protocol, in the **Settings** section:

1. Select the **Enable NFS** option.
2. Optionally, in the **UID** field, type a different UID to be displayed for objects that don't have an explicit POSIX UID. Valid values are integers greater than or equal to zero.

3. Optionally, in the **GID** field, type a different GID to be displayed for objects that don't have an explicit POSIX GID. Valid values are integers greater than or equal to zero.
4. Click on the **Update Settings** button.

#### **Allowed IP Addresses section**

To set the IP addresses to be allowed access to the namespace through NFS, optionally, specify IP addresses in the **Allowed IP Addresses** section. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.

## Configuring the SMTP protocol

With the SMTP protocol, HCP can automatically archive emails forwarded by email servers.

### SMTP protocol configuration

You use the **SMTP** panel to enable and configure the SMTP protocol for a namespace. To display this panel, on the left side of the **Protocols** page, click on **SMTP**.

The top of the **SMTP** panel shows the string to use to identify the namespace when configuring Microsoft® Exchange to archive email to the namespace.

The **SMTP** panel lets you:

- Enable the SMTP protocol
- Specify the email server IP addresses that have access to the namespace through SMTP
- Specify where and in what format email objects are stored
- Specify whether to store email attachments separately

The SMTP protocol always stores attachments along with the email they accompany. The HDDS and HCP search facilities and the metadata query engine index the attachments along with the email.

You can choose to additionally store attachments separately from the email they accompany. With this option, searches return not only the original email with the attachments but also the attachments as separate objects.

When attachments are stored only with the email they accompany, searches return only the email objects. You then need to retrieve the email objects and separate the attachments yourself.

Storing attachments as separate objects can have a significant impact on performance and storage space.

## Enabling SMTP access to a namespace

The **SMTP** panel has three sections for enabling and configuring the SMTP protocol.

### Settings section

To enable the SMTP protocol, in the **Settings** section:

1. Select the **Enable SMTP** option.
2. Click on the **Update Settings** button in the **Settings** section.

### Allow/Deny section

Optionally, in the **Allow/Deny** section, specify IP addresses of email servers to be allowed or denied access to the namespace through SMTP. For instructions on doing this, see [“Adding and removing entries in Allow and Deny lists”](#) on page 182.

For information on how HCP handles IP addresses that appear in both or neither of the **Allow** and **Deny** lists, see [“Allow and Deny list handling for CIFS”](#) on page 184.

### Emails section

To set options specific to email objects:

1. Click on **Emails**.
2. In the **Emails** section:
  - In the **Email Location** field, type the path for the directory in which you want email objects stored. This is the full path starting after the root directory (that is, `rest` or `data`). Be sure to start and end the path with a forward slash (`/`), like this:

`/email/company_all/`

If any part of the specified directory path doesn't exist, HCP creates it.

For information on the complete path and object names for email added to the namespace through SMTP, see *Using a Namespace*.

- In the **Format** field, select either **.eml** or **.mbox**. The one you choose depends on the application you use to read the stored email.
- To store email attachments separately from the emails they're attached to, select the **Separate attachments from parent email** option. For more information on storing email attachments, see ["SMTP protocol configuration"](#) on page 196.



---

**Important:** Storing attachments separately from the email they accompany can have a significant impact on performance and storage space. Unless you have a specific reason to do so, do not enable this option.

---

3. Click on the **Update Settings** button in the **Emails** section.

## Configuring Microsoft Exchange for email archiving through SMTP

HCP provides SMTP support for Microsoft Exchange 2003, 2007, and 2010 email servers. The following sections outline the procedures for configuring each supported version of Exchange for email archiving through SMTP.

For considerations that apply to configuring Exchange 2003 and 2010 in an environment that uses both versions, see "Exchange 2003 and Exchange 2010 Journaling Interoperability"

(<http://technet.microsoft.com/en-us/library/aa997918.aspx#Exc>).



---

**Note:** HCP supports archiving email to multiple namespaces. However, with Microsoft Exchange 2003, the recommendation is to archive email to only one namespace.

---

### Configuring Microsoft Exchange 2003

To configure Microsoft Exchange 2003 for archiving emails to an HCP namespace through SMTP:

1. Create a custom SMTP recipient, using a name that's unique for the namespace. For the recipient email address, use *username@namespace-name.tenant-name.hcp-domain-name*, where *username* is the username of any new or existing user (for example, *admin@accounts-receivable.finance.hcp.example.com*). For the new email address type, select **SMTP Address**.

For details, see “How to Create a Custom SMTP Recipient for Exchange Server 2003 Journaling”

(<http://technet.microsoft.com/en-us/library/bb124642%28EXCHG.65%29.aspx>).




---

**Note:** You need to create a separate custom SMTP recipient for each namespace to which you want to archive email.

---

2. Create journal recipient mailboxes. For details, see “Planning an Exchange Server 2003 Journaling Deployment”  
(<http://technet.microsoft.com/en-us/library/aa998762%28EXCHG.65%29.aspx>).




---

**Tip:** For better performance, create the journal recipient mailboxes on separate servers from the user mailbox servers.

---

3. Define a server-side forwarding rule for the journal recipient mailboxes. For details, see “How to Set a Server-Side Rule for Journal Recipient Mailboxes”  
(<http://technet.microsoft.com/en-us/library/bb124633%28EXCHG.65%29.aspx>).
4. Configure Exchange Mailbox Manager to clean out the journal recipient mailboxes after the journalized messages in them are transmitted. For details, see “How to Configure Mailbox Manager to Clean the Journal Recipient Mailbox”  
(<http://technet.microsoft.com/en-us/library/aa995756%28EXCHG.65%29.aspx>).
5. Configure the Exchange server SMTP protocol for the target namespace, creating a new virtual SMTP server with a unique IP address. For both the fully qualified domain name and masquerade domain, specify  
*www.namespace-name.tenant-name.hcp-domain-name*.

For details, see “How to Configure External DNS Servers on an Outbound SMTP Virtual Server”

(<http://technet.microsoft.com/en-us/library/bb124221%28EXCHG.65%29.aspx>).

6. Configure a dedicated SMTP connector to transmit journalized messages to *smtp.hcp-domain-name*. For details, see “How to Create an SMTP Connector”  
(<http://technet.microsoft.com/en-us/library/aa996625%28EXCHG.65%29.aspx>).

7. For each mailbox store, enable standard journaling. For details, see “How to Enable Standard Journaling” (<http://technet.microsoft.com/en-us/library/bb124786%28EXCHG.65%29.aspx>).
8. Enable envelope journaling. For details, see “How to Enable Envelope Journaling” (<http://technet.microsoft.com/en-us/library/aa997541%28EXCHG.65%29.aspx>).

For additional information on this procedure, see “Implementing Exchange 2003 Message Journaling” (<http://www.msexchange.org/tutorials/Implementing-Exchange-2003-Messaging-Journaling.html>).

## Configuring Microsoft Exchange 2007

To configure Microsoft Exchange 2007 for archiving emails to an HCP namespace through SMTP:

1. Create a custom SMTP recipient, using a name that’s unique for the namespace. For the recipient email address, use *username@namespace-name.tenant-name.hcp-domain-name*, where *username* is the username of any new or existing user (for example, *admin@accounts-receivable.finance.hcp.example.com*).

For details, see “How to Create a New Mail Contact” ([http://technet.microsoft.com/en-us/library/aa997220\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa997220(EXCHG.80).aspx)).



---

**Note:** You need to create a separate custom SMTP recipient for each namespace to which you want to archive email.

---

2. Create the mailboxes to be journaled. For details, see “How to Create a Mailbox for a New User” ([http://technet.microsoft.com/en-us/library/aa998197\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998197(EXCHG.80).aspx)).



---

**Tip:** For better performance, create the journal mailboxes on separate servers from the user mailbox servers.

---

3. Create a custom Send connector for the Exchange server. For the address space, use *namespace-name.tenant-name.hcp-domain-name*. Choose smart host for email routing. For details, see “How to Create a



New Send Connector”

([http://technet.microsoft.com/en-us/library/aa998814\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa998814(EXCHG.80).aspx)).




---

**Note:** You need to create a separate custom Send connector for each namespace to which you want to archive email.

---

4. Modify the custom Send connector for the target namespace. For the fully qualified domain name to be returned in response to the EHLO command, specify *namespace-name.tenant-name.hcp-domain-name*. For details, see “How to Modify the Configuration of a Send Connector” (<http://technet.microsoft.com/en-us/library/aa998836%28EXCHG.80%29.aspx>).
5. Create a journal rule to send journal reports to the custom SMTP recipient you created in [step 1](#) above. For details, see “How to Create a New Journal Rule” ([http://technet.microsoft.com/en-us/library/bb124723\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb124723(EXCHG.80).aspx)).

## Configuring Microsoft Exchange 2010

To configure Microsoft Exchange 2010 for archiving emails to an HCP namespace through SMTP:

1. Create the user mailboxes to be journaled and, optionally, a new user for each mailbox, using a name that’s unique for the namespace. For the user email address, use *username@namespace-name.tenant-name.hcp-domain-name*, where *username* is the username of any new or existing user (for example, *admin@accounts-receivable.finance.hcp.example.com*).

For details, see “Create a Mailbox”

(<http://technet.microsoft.com/en-us/library/bb123809.aspx>).

2. Create a new SMTP Send connector for the Exchange server. For the address space, use *namespace-name.tenant-name.hcp-domain-name*. For the smart host authentication settings, select **None**. For details, see “Create an SMTP Send Connector” (<http://technet.microsoft.com/en-us/library/aa997285.aspx>).




---

**Note:** You need to create a separate custom Send connector for each namespace to which you want to archive email.

---

3. Modify the custom Send connector for the target namespace. For the fully qualified domain name to be returned in response to the EHLO command, specify *namespace-name.tenant-name.hcp-domain-name*. For details, see “Configure Send Connector Properties” (<http://technet.microsoft.com/en-us/library/bb629503.aspx>).
4. Optionally, if you have the Enterprise edition of Microsoft Exchange 2010, create a journal rule to selectively journal emails. For details, see “Create a Journal Rule” (<http://technet.microsoft.com/en-us/library/aa995915.aspx>).

# Managing search and indexing

You manage search and indexing for namespaces at both the tenant and namespace level. At the tenant level, you create content classes and content properties. At the namespace level, you enable search and indexing options.

This chapter contains:

- An overview of search and indexing
- An explanation of content classes and content properties and instructions for working with them
- Instructions for managing search and indexing for individual namespaces



---

**Note:** The discussion of content properties in this chapter assumes a basic understanding of XML.

---

## About search and indexing

For a namespace to be searchable through either the metadata query API or the Search Console, it must be search enabled, and its effective permission mask must include the read and search permissions. Additionally, to get results from object-based queries through the metadata query API and from searches through the Search Console with any search facility, the namespace must be indexed by the applicable search facility.

You can enable search for your namespaces only if allowed to do so by the tenant configuration. HCP system-level administrators can change this configuration from not allowing you to enable search to allowing it. However, they cannot do the reverse.

### **Metadata query engine and HCP search facility indexing**

The metadata query engine and the HCP search facility index each namespace that has both search and indexing enabled. When you first enable search for a namespace, indexing is enabled by default.

The metadata query engine index is based on system metadata, ACLs, and, optionally, custom metadata that is well-formed XML. The HCP search facility index is based on object data, system metadata, and, optionally, custom metadata.

You can enable or disable indexing for a namespace at any time while search is enabled for the namespace. Disabling indexing for a namespace prevents the metadata query engine and HCP search facility from updating their indexes with new objects and metadata changes in that namespace. When indexing is reenabled, these facilities update their indexes with the backlogged objects and changes and continue indexing from there.

You can enable or disable indexing of custom metadata for a namespace at any time while indexing is enabled for the namespace. Because indexing custom metadata can significantly increase the size of the indexes, you should enable it only if users need to perform searches based on custom metadata.

Indexing can be disabled for the metadata query engine or HCP search facility at the HCP system level. If this indexing is disabled at the system level, enabling it at the namespace level has no effect.

Similarly, custom metadata indexing can be disabled for the metadata query engine or HCP search facility at the HCP system level. If this indexing is disabled at the system level, enabling it at the namespace level has no effect.

You can reduce the amount of custom metadata the metadata query engine indexes by creating content properties. Content properties not only decrease the size of the index but also enable users to query for objects more easily and intuitively. For information on content properties, see [“Content classes and content properties”](#) on page 206.

You can also reduce the size of the metadata query engine index by excluding selected custom metadata annotations from being indexed.

Content properties and annotation exclusions affect only metadata query engine indexing. They have no effect on HDDS and HCP search facility indexing.




---

**Note:** When indexing custom metadata, the HCP search facility indexes only annotations named default.

---

For an introduction to the metadata query engine and HCP search facility, see [“HCP Search Console”](#) on page 7. For information on annotations, see *Using a Namespace*.

### **HDDS search facility indexing**

The HDDS search facility indexes objects in a namespace only while all of these are true:

- Search is enabled for the namespace.
- HTTP is enabled for the namespace.
- The effective permission mask for the namespace includes the read and search permissions.
- The HCP management API is enabled at both the system level and tenant levels.
- The HCP system uses DNS for system addressing.
- The namespace is known to HDDS.

For an introduction to the HDDS search facility, see [“HCP Search Console”](#) on page 7.

### **Disabling search**

You can disable and reenable search for a namespace at any time. When you disable search, indexing is automatically disabled for all three search facilities.

Disabling search also removes objects in the namespace from the metadata query engine and HCP search facility indexes. If you subsequently reenables search for the namespace, the namespace must be completely reindexed. The amount of time required to rebuild the indexes depends on the amount of data in the namespace. With a very large amount of data, this process can take several days.

## Content classes and content properties

A **content class** is a named construct that is used to characterize objects in one or more namespaces. Content classes use object metadata to impose structure on unstructured namespace content. They do this through content properties.

A **content property** is a named construct used to extract an element or attribute value from custom metadata that's well-formed XML. Content properties use XPath expressions to identify the metadata of interest. When content properties are indexed, users can use them to find unstructured content that matches structured patterns.

For example, consider the following XML structure that could occur in the custom metadata for multiple objects in a namespace that contains medical data:

```
<doctor>
  <name>doctor-name</name>
</doctor>
<patient>
  <name>patient-name</name>
</patient>
```

The information of interest in this custom metadata consists of the doctor's name and the patient's name.

Based on the metadata structure above, you could create content properties named `Doctor_Name` and `Patient_Name` that extract the doctor's name and patient's name from the custom metadata XML for each object. The metadata query engine could then index objects with this metadata structure by those property values. Using the metadata query API or the Metadata Query Engine Console, users could query for objects that have `Doctor_Name` or `Patient_Name` equal to a specific value.

Content properties belong to content classes. Both content classes and content properties are defined at the tenant level. Content classes are optionally associated with namespaces. Through this association, content properties are associated with namespaces.

## Metadata query engine indexing of custom metadata

By default, when custom metadata indexing is enabled for a namespace, the metadata query engine indexes the content properties for that namespace and not the full text of custom metadata. If the namespace doesn't have any content properties (that is, it's not associated with any content classes that have content properties), no custom metadata is indexed.

You can choose to have the metadata query engine index the full text of custom metadata. If you enable this option, the metadata query engine indexes both content properties, if any exist, and the full text of custom metadata.

With content properties, the metadata query engine indexes only the values that you determine are of interest. When indexing the full text of custom metadata, the metadata query engine indexes each word individually.

For example, suppose an object has this XML in its custom metadata:

```
<doctor>
  <name>Lee Green</name>
</doctor>
<patient>
  <name>Paris Black</name>
</patient>
```

If you've defined the Doctor\_Name and Patient\_Name properties, the metadata query engine index includes:

```
Lee Green
Paris Black
```

If full text indexing is enabled, the metadata query engine index includes:

```
doctor name Lee Green name doctor patient name Paris Black name patient
```

In this case, to use the metadata query API to find the objects that have a doctor named Lee Green, users would need to query for custom metadata containing "doctor.name.Lee Green.name.doctor". This kind of query can become very complex when elements are nested to deeper levels or when they have attributes.

## Content class and content property workflow

Here's the basic procedure for working with content classes and content properties:

1. Create one or more content classes for the tenant. Give each class a meaningful name. For example, if a class will contain object properties that pertain to medical images, you could name it DICOM. (DICOM is a standard for managing medical images.)

A tenant can have at most 25 content classes.

For more information, see [“Creating a content class”](#) on page 228.

2. Create content properties for each content class. Create only the content properties that will be useful to metadata query API and Search Console users. Creating content properties that won't be used unnecessarily increases the size of the metadata query engine index.

A content class can have at most 100 content properties.

For more information, see [“Content property definitions”](#) below and [“Managing content properties for a content class”](#) on page 228.

3. If custom metadata indexing isn't already enabled for the namespaces you plan to associate with the content classes, enable it. For more information, see [“Setting search and indexing options”](#) on page 238.
4. Associate namespaces with the applicable content classes. For clarity, associate a namespace with a content class only if the namespace contains objects that can be characterized by the content properties in the content class.

You can associate any number of namespaces with a content class. Additionally, a namespace can be associated with any number of content classes.

For more information, see [“Changing the namespaces associated with a content class”](#) on page 232.

5. Optionally, reindex some or all of the namespaces associated with the content classes. You would reindex a namespace if you want objects that were already in the namespace to be indexed by the new content properties.



You can reindex namespaces starting from the time they were created or starting from a specific date. When reindexing a namespace, the metadata query engine reindexes all objects with a change time that's equal to or later than the time you specify.



---

**Tip:** Because reindexing can take a long time, before reindexing a namespace:

- Create all the content properties you want for the namespace
  - Associate all the content classes containing those properties with the namespace
- 

For more information, see [“Reindexing namespaces associated with a content class”](#) on page 233 and [“Reindexing an individual namespace”](#) on page 239.

## Content property definitions

The definition of a content property consists of:

- A name for the property.
- The XPath expression that identifies the property values.
- The data type of the property values.
- For numeric and datetime data types, the format of the property values.
- An indication of whether the property is single-valued or multivalued. A multivalued property can have multiple values for any given object.

The examples of content property definitions in the following sections are based on this sample custom metadata XML:

```
<?xml version="1.0" ?>
<dicom_image>
  <image type="MRI">
    <date>09/27/2012</date>
    <technician>Morgan Grey</technician>
  </image>
  <doctor>
    <name>Lee Green</name>
    <office>ABC Oncology</office>
    <address>
      <address1>Anytown Medical Building</address1>
      <address2>1 Main Street</address2>
      <city>Anytown</city>
      <state>MA</state>
      <zip>02000</zip>
    </address>
    <specialties>
      <specialty primary="true">Oncology</specialty>
      <specialty>Internal Medicine</specialty>
    </specialties>
  </doctor>
  <patient>
    <id>243789</id>
    <name>Paris Black</name>
    <address>
      <address1>10 Elm Street</address1>
      <address2/>
      <city>Anytown</city>
      <state>MA</state>
      <zip>02000</zip>
    </address>
  </patient>
  <followup_needed>true</followup_needed>
</dicom_image>
```

## Content property names

When you define a content property, you specify a name for it. Content property names must be from one through 25 characters long, can contain only alphanumeric characters and underscores (\_), and are case sensitive. White space is not allowed.

Content property names should be intuitive for users of the metadata query API and Metadata Query Engine Console. For example, for the property that extracts the name of the doctor from the sample custom metadata, you should use a name like `Doctor_Name` rather than a name like `dname`.

### Content properties with the same name

You can use the same name for multiple content properties as long as those properties have the same data type. For example, suppose the custom metadata for some objects includes a **physician** element instead of a **doctor** element, like this:

```
<physician>
  <name>Lee Green</name>
  <office>ABC Oncology</office>
  <address>
    <address1>Anytown Medical Building</address1>
    <address2>1 Main Street</address2>
    <city>Anytown</city>
    <state>MA</state>
    <zip>02000</zip>
  </address>
  <specialties>
    <specialty primary="true">Oncology</specialty>
    <specialty>Internal Medicine</specialty>
  </specialties>
</physician>
```

You could define two content properties named `Doctor_Name`, one with an XPath expression that includes the **doctor** element, the other with an XPath expression that includes the **physician** element.

Within a content class, content properties with the same name must have the same data type. For information on data types, see [“Content property data types”](#) on page 215.

### Reserved words

The following words are reserved and cannot be used as content property names:

- accessTime
- accessTimeString
- acl
- changeTimeMilliseconds
- changeTimeString
- customMetadata
- customMetadataAnnotation
- dpl
- gid
- hash
- hashScheme
- hold
- index
- ingestTime
- ingestTimeString
- namespace
- objectPath
- operation
- owner
- permission
- replicated
- retention
- retentionClass
- retentionString
- shred
- size
- type
- uid
- urlName
- updateTime
- updateTimeString
- utf8Name
- version

### Content property expressions

For each content property you create, you specify an XPath expression. An XPath expression is an instruction for navigating an XML document to find an element or attribute value.

XPath expressions use the XPath language. HCP supports the full syntax of this language. The examples in this section illustrate only a small part of the XPath syntax.

You can learn more about XPath expressions at:

<http://www.w3schools.com/xpath>

### **XPath expressions that find element values**

Here's a simple XPath expression that finds the value of the **followup\_needed** element:

```
/dicom_image/followup_needed
```

The forward slash (/) at the beginning of the expression means that the first element is the root element in the XML. The element after the second forward slash is a child of the root element.

Here's another simple XPath expression:

```
//name
```

This expression is probably not very useful. The double slash at the beginning means find the value of any **name** element, regardless of whether that element is a child of the **doctor** element or the **patient** element.

A more useful XPath expression specifies a path to the **name** element:

```
/dicom_image/doctor/name
```

This expression means start at the root element, find the **doctor** element that's the child of the root element, and then find the **name** element that's the child of the **doctor** element. A content property with this expression finds only the name of the doctor, not the name of the patient.

A different content property with this Xpath expression finds only the patient's name:

```
/dicom_image/patient/name
```

The element path in an XPath expression can go deeper than the three levels shown above. Here's an XPath expression that's four levels deep and finds the city in which the doctor's office is located:

```
/dicom_image/doctor/address/city
```

**XPath expressions that find attribute values**

To find the value of an attribute, you include an at sign (@) followed by the attribute name at the end of the XPath expression. For example, here's an XPath expression that finds the value of the **type** attribute of the **image** element:

```
/dicom_image/image@type
```

**Complex XPath expressions**

XPath expressions can be much more complex than the ones shown so far. For example, an XPath expression can navigate XML based on the values of elements and attributes. Here's an expression that finds the name of a doctor whose primary specialty is oncology:

```
/dicom_image/doctor/specialties/specialty[@primary='true' and text()='Oncology']/
  ancestor::doctor/name
```

This expression navigates down from the **doctor** element to the **specialty** elements and finds the one that has both a value of Oncology and a **primary** attribute with a value of true. The expression then navigates back up to the same **doctor** element and from there down to the **name** element that's the child of the **doctor** element.

**Annotation-specific content properties**

You can associate content properties with annotation names. When a content property is associated with an annotation name, the metadata query engine indexes the value of that property only when the value occurs in an annotation with the specified name.

To associate a content property with an annotation name, you specify the case-sensitive annotation name in front of the XPath expression for the property, in this format:

```
@annotation-name:xpath-expression
```

For example, suppose:

- The objects in a namespace can have either of two annotations — one named **dicom**, the other named **appointment**
- Both of these annotations have a **date** element
- Depending on who created the **dicom** annotation, the **date** element in it might be a child of the root element or a child of the **image** element

To find the value of the **date** element in the dicom annotation, you would need to use this XPath expression:

```
//date
```

This expression means find a **date** element that occurs anywhere in the XML. Without more context, it applies equally to the dicom and appointment annotations.

To have the content property with this XPath expression apply only to the dicom annotation, you would specify the expression this way:

```
@dicom://date
```

## Content property data types

Each content property has a data type that determines how the property values are treated by the metadata query engine. The possible data types are:

- **String** — The metadata query engine indexes the value as a text string. The value is handled as a single unit, even if it contains white space. Users cannot base queries on individual terms within a string value.
- **Tokenized** — The metadata query engine indexes the value as a text string after breaking it into tokens. A token is a string of either alphabetic or numeric characters. For example, the value *SSN12345789* becomes this string of two tokens: *ssn 123456789*. Tokens are not case sensitive.

The metadata query engine treats white space and special characters as token separators. For example, the value *12A Elm Street, apt. 2D* becomes this string of seven tokens: *12 a elm street apt 2 d*.

Users can base queries on any individual token or sequence of tokens within a tokenized string.

- **Boolean** — The metadata query engine indexes the value as true or false. Values that start with *1*, *t*, or *T* are treated as true. Any other values are treated as false.
- **Integer** — The metadata query engine indexes the value as an integer. Users can base queries on comparative numeric values.

The metadata query engine indexes values for a content property with a data type of integer only if the values conform to the format for the property. For more information, see ["Formats for the integer and float data types"](#) below.

- **Float** — The metadata query engine indexes the value as a decimal number with or without an exponent, depending on the value. Users can base queries on comparative numeric values.

The metadata query engine indexes values for a content property with a data type of float only if the values conform to the format for the property. For more information, see ["Datetime data type formats"](#) on page 219.

- **Datetime** — The metadata query engine indexes the value as a date and time. Users can base queries on comparative datetime values.

The metadata query engine indexes values for a content property with a data type of date only if the values conform to the format for the property. For more information, see ["Datetime data type formats"](#) on page 219.

## Formats for the integer and float data types

For a content property with the integer or float data type, you can specify a format that values need to match in order to be indexed. The following sections include basic information about these formats. You can find more information at:

<http://docs.oracle.com/javase/6/docs/api/java/text/DecimalFormat.html>

### Integer data type formats

The basic format for a content property with the integer data type is:

*optional-prefix number-pattern optional-suffix*

A number pattern for the integer data type consists of any number of number signs (#), followed by any number of zeroes. Both number signs and zeroes represent any number of digits, including none. The metadata query engine does not consider the length of the number pattern when matching values.

A number pattern can include a thousands separator. With the integer data type, the metadata query engine recognizes either commas (,) or periods (.) as the thousands separator.



For example, a value of *1234* matches any of these number patterns:

```
0
000
##
###0000
0,0
##,000
```

If a content property value contains a thousands separator, the value matches only number patterns that contain the same thousands separator. For example, the value *1,234* matches the last two patterns above, but not the first four. It also does not match *0.0* or *##.000*.

The prefix or suffix in the format for the integer data type can be any character string, with a few exceptions. For example, a prefix or suffix cannot include a period (.) or percent sign (%). The format must include white space between the integer pattern and the suffix, if used.

For example, for the metadata query engine to index the value *\$1234* as an integer, the format for the content property must have a dollar sign (\$) in front of the integer pattern, with no space between them.

Here are some examples of integer formats with examples of values that match them:

Format	Example
\$ 0,0	\$ 1,234
###0 AD	2012 AD
~# mph	~55 mph

If you don't specify a format for a content property with the integer data type, the metadata query engine indexes only sequences of digits with no special characters.

### Float data type formats

For the format for a content property with the float data type, you can use any of the formats for the integer data type. However, with the float data type, the thousands separator, if used, must be a comma (,).

You can include a period as a decimal separator in the number pattern for the float data type, although this is not required. If you do include it, any number signs (#) must come after any zeroes in the part following separator.

For example, a value of *1234.5* matches any of these number patterns:

```
0
00.0
.0
#0.0#
##,000
0,0
#,0.0#
```

You can also include an exponent character (E) followed by one or more zeroes in the number pattern for the float data type. However, values with an exponent character also match patterns that don't include the exponent character, and values without an exponent character also match patterns with an exponent character.

For example, a value of *1234E5* matches any of these number patterns:

```
0
00.0
.0E0
#0.0#E000
##,000E0
0,0
#,0.0E00
```

You can use a percent sign (%) by itself as the prefix or suffix in the format for the float data type. Before indexing values with a matching percent sign, the metadata query engine converts them to their decimal equivalents. For example, a value of *1234%* matches a format of *0%* and is indexed as *12.34*.

White space is not required between the number pattern and a suffix that's a percent sign.

If you don't specify a format for a float data type, the metadata query engine indexes only sequences of digits that optionally include one decimal point.

## Datetime data type formats

For a content property with the datetime data type, you can specify a format that values need to match in order to be indexed. The format consists of a pattern of letters, optional separators, and optional quoted text. The letters represent date or time components, as outlined in the table below. Letters can be repeated, which can affect their meaning.

Letter	Description
G	Represents a valid era indicator, such as AD, BC, or BCE. Repetition has no effect.  If a datetime pattern doesn't include any occurrences of G, the metadata query engine assumes an era of AD for matching values.
y	Represents a year. For matching values with a two-digit year, a pattern that includes y more than twice in a row causes the metadata query engine to interpret the two digits as being preceded by two zeroes rather than by the number that indicates the current century.  If a datetime pattern doesn't include any occurrences of y, the metadata query engine assumes a year of 1970 for matching values.
M	Represents a month. Values that include the month as a number match a pattern that includes M or MM. Values that include the name of the month, either in full or as a three-letter abbreviation, match a pattern that includes three or more occurrences of M in a row.  If a datetime pattern doesn't include any occurrences of M, the metadata query engine assumes a month of January for matching values.
w	Represents the number of the week into the year. Repetition has no effect.
W	Represents the number of the week into the month, where the first week is the week that includes the first day of the month. Repetition has no effect.
D	Represents the number of the day into the year. Repetition has no effect.
d	Represents the number of the day into the month. Repetition has no effect.
F	Represents the number of the week into the month, where the first week starts with the first Sunday in the month. Repetition has no effect.
E	Represents the day of the week. Matching values include the name of the day in full or as a three-letter abbreviation. Repetition has no effect.
a	Represents a valid morning or afternoon indicator, such as AM or pm. Repetition has no effect.
H	Represents the hour on a 24-hour clock, where midnight is represented by zero. Repetition has no effect.
k	Represents the hour on a 24-hour clock, where midnight is represented by 24. Repetition has no effect.

*(Continued)*

Letter	Description
K	Represents the hour on a 12-hour clock, where midnight and noon are represented by zero. Repetition has no effect.
h	Represents the hour on a 12-hour clock, where midnight and noon are represented by 12. Repetition has no effect.
m	Represents the minute into the hour. Repetition has no effect.  If a datetime pattern doesn't include any occurrences of m, the metadata query engine assumes that the number of minutes is zero for matching values.
s	Represents the second into the minute. Repetition has no effect.  If a datetime pattern doesn't include any occurrences of s, the metadata query engine assumes that the number of seconds is zero for matching values.
S	Represents a number of milliseconds past the applicable second. Repetition has no effect.
z	Represents a valid time zone specified as text, such Eastern Standard Time, EDT, or GMT. Repetition has no effect.
Z	Represents a valid time zone specified as an offset from GMT, formatted as (+ -)nnnn, such as +0500 or -0200. Repetition has no effect.

If a datetime format doesn't include a representation for:

- A day, the metadata query engine assumes that the day is the first day of the applicable month for matching values
- An hour, the metadata query engine assumes that the hour is midnight
- A time zone, the metadata query engine assumes that the time is in the HCP system time zone

The separators in a datetime format can be any of several different special characters, including forward slashes (/), hyphens (-), colons (:), semicolons (;), at signs (@), and spaces.

To include text in a datetime format, enclose the text in single quotation marks ('). To include a single quotation mark, specify two single quotation marks in a row.

Here are some examples of datetime formats with examples of values that match them:

Format	Example
MM/dd/yy HH:mm:ss z	03/19/12 14:35:27 EST
hh 'o'clock' a, zzz	2 o'clock PM, Eastern Standard Time
yyyy-MM-dd'T'HH:mm:ss.SSSZ	2012-03-19T14:35:27.236-0400
E., MMM d, yyyy 'at' k:s	Mon., March 19, 2012 at 14:35

If you don't specify a format for a content property with the datetime data type, the metadata query engine indexes only values that match patterns such as MM/dd/yyyy, MM-dd-yyyy, yyyy-MM-dd, or yyyy-MM-dd'T'HH:mm:ssZ.

You can find more information about datetime formats at:

<http://docs.oracle.com/javase/6/docs/api/java/text/SimpleDateFormat.html>

## Multivalued content properties

A content property is defined as either single-valued or multivalued:

- If you define a content property as single-valued, the metadata query engine indexes only the first occurrence of it for any given object, regardless of how many times it occurs in the custom metadata XML for that object.
- If you define a content property as multivalued, the metadata query engine indexes all occurrences of it in the custom metadata XML for an object.

For example, based on the sample custom metadata XML, you would define as multivalued a content property that extracts the value of the **specialty** element.

With the metadata query API, users can sort query results based on single-valued content properties but not on multivalued properties.

## Content properties extracted from sample XML

When working with content properties in the Tenant Management Console, you can supply sample well-formed XML and have HCP extract content properties from that XML. You can then select which of those properties you want to add to a content class.

HCP extracts only content properties for XPath expressions that follow a straight path from the root element. These conventions apply to the content property definitions:

- The XPath expression always starts from the root element.
- The name of a content property that extracts an element value is the name of the element preceded by the name of the parent element.
- The name of a content property that extracts an attribute value is the name of the attribute preceded by the name of the element the attribute applies to.
- Content property names that would exceed 25 characters in length are truncated to 25 characters, starting from the beginning.
- The definitions do not include formats.
- The definitions are listed alphabetically by XPath expression.

When adding extracted content properties to a content class, you can change any parts of their definitions.

The table below shows the definitions of the content properties HCP extracts from the sample custom metadata XML.

XPath expression	Name	Data Type	Multivalued
/dicom_image/doctor/address/address1	addressAddress1	String	No
/dicom_image/doctor/address/address2	addressAddress2	String	No
/dicom_image/doctor/address/city	addressCity	String	No
/dicom_image/doctor/address/state	addressState	String	No
/dicom_image/doctor/address/zip	addressZip	Integer	No
/dicom_image/doctor/name	doctorName	String	No
/dicom_image/doctor/office	doctorOffice	String	No
/dicom_image/doctor/specialties/specialty	specialtiesSpecialty	String	Yes
/dicom_image/doctor/specialties/specialty/@primary	specialtyPrimary	Boolean	No
/dicom_image/followup_needed	icom_imageFollowup_needed	Boolean	No
/dicom_image/image/@type	imageType	String	No
/dicom_image/image/date	imageDate	String	No

*(Continued)*

XPath expression	Name	Data Type	Multivalued
/dicom_image/image/technician	imageTechnician	String	No
/dicom_image/patient/address/address1	addressAddress1	String	No
/dicom_image/patient/address/address2	addressAddress2	String	No
/dicom_image/patient/address/city	addressCity	String	No
/dicom_image/patient/address/state	addressState	String	No
/dicom_image/patient/address/zip	addressZip	Integer	No
/dicom_image/patient/id	patientId	Integer	No
/dicom_image/patient/name	patientName	String	No

## Content property files

You can export the content properties for a content class to a file that you can then use to import the properties to another class. The exported file contains XML definitions of the content properties in this format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<contentClass>
  <contentProperties>
    <contentProperty>
      <name>property-name</name>
      <expression>xpath-expression</expression>
      <type>data-type</type>
      <multivalued>true-or-false</multivalued>
      <format>format</format>
    </contentProperty>
    .
    .
    .
  </contentProperties>
</contentClass>
```

Using the same format, you can also create content property files yourself.

Here's an example of XML that defines some content properties based on the sample custom metadata XML:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<contentClass>
  <contentProperties>
    <contentProperty>
      <name>Doctor_City</name>
      <expression>/dicom_image/doctor/address/city</expression>
      <type>STRING</type>
      <multivalued>>false</multivalued>
      <format />
    </contentProperty>
    <contentProperty>
      <name>Doctor_State</name>
      <expression>/dicom_image/doctor/address/state</expression>
      <type>STRING</type>
      <multivalued>>false</multivalued>
      <format />
    </contentProperty>
    <contentProperty>
      <name>Doctor_Name</name>
      <expression>/dicom_image/doctor/name</expression>
      <type>STRING</type>
      <multivalued>>false</multivalued>
      <format />
    </contentProperty>
    <contentProperty>
      <name>Doctor_Office</name>
      <expression>/dicom_image/doctor/office</expression>
      <type>STRING</type>
      <multivalued>>false</multivalued>
      <format />
    </contentProperty>
    <contentProperty>
      <name>Doctor_Specialty</name>
      <expression>/dicom_image/doctor/specialties/specialty</expression>
      <type>STRING</type>
      <multivalued>>true</multivalued>
      <format />
    </contentProperty>
    <contentProperty>
      <name>Followup_Needed</name>
      <expression>/dicom_image/followup_needed</expression>
      <type>BOOLEAN</type>
      <multivalued>>false</multivalued>
      <format />
    </contentProperty>
  </contentProperties>
</contentClass>
```



```

    <name>Image_Type</name>
    <expression>/dicom_image/image/@type</expression>
    <type>STRING</type>
    <multivalued>>false</multivalued>
    <format />
  </contentProperty>
  <contentProperty>
    <name>Image_Date</name>
    <expression>/dicom_image/image/date</expression>
    <type>DATE</type>
    <multivalued>>false</multivalued>
    <format>MM/dd/yyyy</format>
  </contentProperty>
  <contentProperty>
    <name>Patient_City</name>
    <expression>/dicom_image/patient/address/city</expression>
    <type>STRING</type>
    <multivalued>>false</multivalued>
    <format />
  </contentProperty>
  <contentProperty>
    <name>Patient_State</name>
    <expression>/dicom_image/patient/address/state</expression>
    <type>STRING</type>
    <multivalued>>false</multivalued>
    <format />
  </contentProperty>
  <contentProperty>
    <name>Patient_ID</name>
    <expression>/dicom_image/patient/id</expression>
    <type>INTEGER</type>
    <multivalued>>false</multivalued>
    <format />
  </contentProperty>
  <contentProperty>
    <name>Patient_Name</name>
    <expression>/dicom_image/patient/name</expression>
    <type>STRING</type>
    <multivalued>>false</multivalued>
    <format />
  </contentProperty>
</contentProperties>
</contentClass>

```

## About the Search page

To manage search and indexing for a tenant, including viewing, creating, and managing content classes and content properties, you use the **Search** page in the Tenant Management Console. To display this page:

1. In the top-level menu, mouse over **Services** to display a secondary menu.
2. In the secondary menu, click on **Search**.



---

**Roles:** To view existing content classes and content properties, you need the monitor or administrator role. To create, modify, and delete content classes and content properties and reindex namespaces associated with content classes, you need the administrator role.

---

## Managing the content class list

The **Search** page lists existing content classes. For each content class, the list shows the content class name.

By default, the content class list includes all existing content classes. The content classes are listed 20 at a time in ascending order by name.

You can page through, sort, and filter the list of content classes. The **Search** page indicates which content classes are shown out of the total number of content classes in the current list.

### Paging

You can change the number of content classes shown at a time on the **Search** page. To do this, in the **Items per page** field, select the number of content classes you want. The options are 10, 20, and 50.

To page forward or backward through the content class list, click on the next (  ) or back (  ) control, respectively.

To jump to a specific page in the content class list:

1. In the **Page** field, type the page number you want.
2. Press Enter.


### Sorting


You can sort the content class list in ascending or descending order by content class name. To change the sort order, click on the **Name** column heading. Each time you click on the column heading, the sort order switches between ascending and descending.

### Filtering

You can filter the content class list by content class name. The filtered list includes only those content classes with a name that begins with or is the same as a specified text string.

To filter the content class list:


1. In the entry field above the list, type the text string you want to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.
2. Click on the find control (  ).

To redisplay the entire list of storage pools after filtering it, click on the clear filter control (  ).

## Understanding the content property list for a content class

To view the content properties defined for a content class, click on the content class name in the content class list. The panel that opens (the **Settings** panel) contains a list of the content properties in that content class. The properties are listed in alphabetical order by name.

For each content property, the list shows:

- **Name** — The content property name
- **Expression** — The XPath expression for the content property, with an annotation prefix if applicable
- **Type** — The data type of the content property
- **Format** — The format for the content property
-  — An indication of whether the content property is multivalued

## Creating a content class

When you create a content class, you can create content properties for it at the same time. Alternatively, you can create a content class with no properties and add properties to it later.

To create a content class, on the **Search** page:

1. Click on **Create Content Class**.
2. In the **Name** field, type a name for the content class. Content class names must be from one through 64 characters long, can contain any valid UTF-8 characters, including white space, and are not case sensitive.
3. Optionally, define one or more content properties to be added to the content class. For instructions on doing this, see [“Adding, modifying, and deleting content properties”](#) below.
4. If you defined content properties in [step 2](#) above, optionally test or export them. For instructions for these actions, see [“Testing content properties”](#) on page 231 and [“Exporting content properties”](#) on page 231.
5. Click on the **Create Content Class** button.

## Managing content properties for a content class

You can add, modify, and delete content properties for a content class at any time. You can also test the properties against XML that you supply. Additionally, you can export the properties to a content property file.

## Adding, modifying, and deleting content properties

To add, modify, or delete content properties for a content class, on the **Search** page:


1. In the list of content classes in the **Settings** panel, click on the name of the content class for which you want to add, modify, or delete content properties.

2. Do one or more of these:

- To add content properties, do one or more of these:
  - Add one or more properties individually (see [“Adding content properties individually”](#) below)
  - Extract one or more properties from XML that you supply (see [“Extracting content properties from sample XML”](#) on page 230)
  - Import properties from a content property file (see [“Importing content properties from a content property file”](#) on page 230)

A row for each new content property appears in the list of content properties for the content class. The row is highlighted in green.

To remove a new row, click on the delete control (  ) for the row.

- To modify a content property, in the row for the property, make the changes you want.
- To delete an existing content property, click on the delete control (  ) for the row containing the property.

The row turns red. To undo the deletion, click again on the delete control.

3. Optionally, test or export all the listed content properties. For instructions for these actions, see [“Testing content properties”](#) on page 231 and [“Exporting content properties”](#) on page 231.

4. Click on the **Update Settings** button.

If you also typed a new name for the content class in the **Name** field, clicking on the **Update Settings** button changes the content class name.

## Adding content properties individually

To add an individual content property to the content property list for a content class:

1. Above the content property list, click on **Add**.
2. In the new row that appears in the content properties list, fill in the definition for the new content property.

## Extracting content properties from sample XML

To extract content properties from sample XML and add them to the content property list for a content class:

1. In the **Sample Custom Metadata** field, type or paste the well-formed XML from which you want to extract properties.
2. Above the content property list, click on **Extract**.

The **Extract Content Properties** window opens. The window lists all the content properties HCP was able to extract from the sample XML.

3. Select each content property you want to add to the content class.

To select all the listed content properties, click in the checkbox at the top of the list. To deselect all the properties after selecting all, click in the checkbox again.

4. Click on the **Add Selected** button.

A row for each content property you selected appears in the list of content properties for the content class.

5. Optionally, modify the definitions of the new content properties.

## Importing content properties from a content property file

To import content properties from a content property file and add them to the content property list for a content class:

1. Above the content property list, click on **Import**.
2. In the **Import Content Properties** window, click on the **Browse** button. Then select the content property file you want.
3. Click on the **Import** button.

A row for each content property defined in the content property file appears in the list of content properties for the content class.

4. Optionally, modify the definitions of the new content properties.

For more information on content property files, see [“Content property files”](#) on page 223.

## Testing content properties

You can test the definitions of the content properties for a content class at any time. You do this by having HCP extract content property values from sample XML that you supply. The test applies to all the content properties in the content property list, including those that have not yet been committed.

To test the definitions of the content properties in the content property list for a content class, on the **Search** page:

1. In the list of content classes, click on the name of the content class with the content properties you want to test.
2. In the **Sample Custom Metadata** field in the **Settings** panel, type or paste the well-formed XML you want to use for the test.
3. Above the content property list, click on **Test**.

HCP extracts the values it can find for the content properties in the content property list. The extracted values appear in the **Test Value** column in the content property list.

## Exporting content properties

You can export the definitions of the content properties for a content class to a content property file at any time. The resulting file includes the definition of each property in the list, including those that have not yet been committed.

To export the definitions of the content properties in the content property list for a content class to a content property file, on the **Search** page:

1. In the list of content classes, click on the name of the content class with the content properties you want to export.
2. Above the content property list in the **Settings** panel, click on **Export**.
3. When prompted, save the content property file to the location of your choice.

For more information on content property files, see [“Content property files”](#) on page 223.

## Changing the namespaces associated with a content class

You can change the associations between namespaces and content classes at any time. However, only namespaces that are search enabled can be associated with content classes.

When you change the namespaces associated with a content class, you have the option of reindexing all the affected namespaces. If you choose to do this, the metadata query engine reindexes each of those namespaces starting from the time the namespace was created.

To change the namespaces associated with a content class, on the **Search** page:

1. In the list of content classes, click on the name of the content class with for which you want to change namespace associations.
2. In the row of tabs below the content class name, click on **Namespaces**.


In the **Namespaces** panel, the **Associate Namespaces with Content Class** section lists namespaces that are enabled for search and are not already associated with the content class.


If any namespaces are already associated with the content class, they are listed in the **Content Class Namespaces** section.

3. Optionally, filter the list of namespaces in the **Associate Namespaces with Content Class** section by namespace name:
  - a. In the **Associate Namespaces with Content Class** field, type a text string to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.

You cannot filter the namespace list while any of the namespaces in it are selected for association.

- b. Click on the find control (  ).


To redisplay the entire list of unassociated namespaces after filtering it, click on the clear filter control (  ).

4. For each namespace you want to associate with the content class, click on the add control (  ) for the namespace in the **Associate Namespaces with Content Class** section.


The row containing the namespace turns green.



To select all the namespaces listed in the **Associate Namespaces with Content Class** list, click on the **Select All** button.

To deselect a namespace, click on the remove control (  ) for it.

To deselect all the selected namespaces, click on the **Clear** button.

5. For each namespace in the **Content Class Namespaces** section that you want to dissociate from the content class, click on the remove control (  ) for the namespace in that section.

The row containing the namespace turns red.

To select all the namespaces listed in the **Content Class Namespaces** section, click on the **Select All** button.

To deselect a namespace, click on the add control (  ) for it.

To deselect all the selected namespaces, click on the **Clear** button.




---

**Tip:** You can filter the list of namespaces in the **Content Class Namespaces** section by namespace name to include only those namespaces you want to remove from replication.

---

6. Optionally, to reindex all the namespaces you are associating with or dissociating from the content class, select the **Reindex all objects in added/removed namespaces** option.
7. Click on the **Update Content Class** button.

## Reindexing namespaces associated with a content class

You can reindex the namespaces associated with a content class at any time. You might do this for example, if you add a new content property to the content class.

To reindex one or more of the namespaces associated with a content class, on the **Search** page:

1. In the list of content classes, click on the name of the content class with the namespaces you want to reindex.
2. In the row of tabs below the content class name, click on **Reindex**.


The **Content Class Namespaces** section in the **Reindex** panel displays a list of the namespaces that are associated with the content class.

3. Optionally, filter the list of namespaces by namespace name:
  - a. In the **Content Class Namespaces** field, type a text string to use as a filter. This string can be up to 64 characters long and can contain any valid UTF-8 characters, including white space. It is not case sensitive.


You cannot filter the namespace list while any of the namespaces in it are selected for reindexing.

- b. Click on the find control (  ).

To redisplay the entire list of namespaces after filtering it, click on the clear filter control (  ).


4. For each namespace you want to reindex, click on the add control (  ) to select the namespace. The namespace row turns green.

To select all the namespaces in the list, click on the **Select All** button.

To deselect a selected namespace, click on the remove control (  ) for the namespace.

To deselect all the namespaces after selecting all, click on the **Clear** button.

5. In the **Reindex Selected Namespaces** section, select either the **All objects** option or the **Objects modified after** option.

If you select the **Objects modified after** option, either type a date in the associated field or click on the calendar control (  ) to select a date. If you type a date, use this format: *mm/dd/yyyy*

If you enter an invalid date using the correct date format, HCP tries to convert it to a real date. For example, if you enter 11/31/2012, HCP converts it to 12/01/2012.

6. Click on the **Reindex Namespaces** button.

If you selected the **All objects** option, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Reindex Objects** button.



**Note:** If indexing is disabled for any of the selected namespaces, the above procedure by itself does not start the reindexing process for them. To start reindexing those namespaces, you need to reenale indexing for them individually. For information on doing that, see [“Setting search and indexing options”](#) on page 238.

For more information on reindexing namespaces, see [“Content class and content property workflow”](#) on page 208. For information on reindexing an individual namespace from the namespace **Search** panel, see [“Reindexing an individual namespace”](#) on page 239.

## Renaming a content class

You can rename a content class at any time. Renaming a content class has no effect on the associations between namespaces and that class.

To rename a content class, on the **Search** page:


1. In the list of content classes, click on the name of the content class you want to rename.
2. In the **Name** field in the **Settings** panel, type a new name for the content class.
3. Click on the **Update Settings** button.

If you also modified the list of content properties for the content class, clicking on the **Update Settings** button commits those changes as well.

## Deleting a content class

You can delete a content class at any time. When you delete a content class, you have the option of reindexing all the namespaces associated with that class. If you choose to do this, the metadata query engine reindexes each of those namespaces starting from the time the namespace was created.

To delete a content class, on the **Search** page:

1. In the list of content classes in the **Settings** panel, click on the delete control (  ) for the content class you want to delete.

2. In response to the confirming message:
  - a. Optionally, to reindex all namespaces associated with the content class you're deleting, select the **Reindex all objects in associated namespaces** option.
  - b. Click on the **Delete** button.

## Managing search and indexing for an individual namespace

You can change the search and indexing settings for an individual namespace at any time. You can:

- Enable or disable search. Disabling search also:
  - Disables all indexing for the namespace
  - Removes the objects in the namespace from the metadata query engine and HCP search facility indexes
  - Deletes the list of excluded annotations for the namespace
  - Deletes all associations the namespace has with any content classes
- If search is enabled:
  - Enable or disable indexing. Disabling indexing also disables custom metadata indexing for the namespace. However, it does not remove objects in the namespace from the indexes.

By default, when you create a namespace with search enabled, indexing is also enabled.

  - Add or delete associations between content classes and the namespace.
- If indexing is enabled, enable or disable indexing of custom metadata. Disabling custom metadata indexing also disables metadata query engine indexing of the full text of custom metadata.

If you disable custom metadata indexing after it has been enabled, custom metadata that has already been indexed is not removed from the index.

By default, when you create a namespace with search enabled, indexing of custom metadata is disabled.

- If indexing of custom metadata is enabled:
  - Enable or disable metadata query engine indexing of the full text of custom metadata. If you disable this option after it has been enabled, custom metadata text that has already been indexed is not removed from the index.




---

**Note:** For namespaces that existed before the HCP system was upgraded from a release earlier than 6.0, if the namespace had custom metadata indexing enabled before the upgrade, it has full-text custom metadata indexing enabled after the upgrade.

---

- Specify annotations to be excluded from metadata query engine indexing of custom metadata. Annotations are excluded by name. So, for example, you could exclude all annotations named *miscellaneous*. Users cannot query for objects based on the content of excluded annotations.

You can also reindex an individual namespace at any time. You might do this, for example, if you associate additional content classes with the namespace.

To manage search and indexing for an individual namespace, you use the namespace **Search** panel in the Tenant Management Console. To display this panel:

1. In the top-level menu, click on **Namespaces**.
2. In the list of namespace on the **Namespaces** page, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Services**.
4. On the left side of the **Services** panel, click on **Search**.

While the metadata query engine or HCP search facility is selected for use with the Search Console, the **Search** panel shows the date and time before which eligible objects in the namespace are guaranteed to be included in the applicable index.



---

**Roles:** To view the search and indexing settings for a namespace, you need the monitor or administrator role. To modify the search and indexing settings for a namespace or to reindex a namespace, you need the administrator role.

---

## Setting search and indexing options

To change the search and indexing options for an individual namespace, in the **Search** panel for the namespace:

1. Optionally, select or deselect the **Enable search** option to enable or disable search, respectively.
2. If the **Enable search** option is selected:
  - Optionally, select or deselect the **Enable indexing** option to enable or disable indexing, respectively.
  - Optionally, in the **Content Classes** list, select or deselect content classes to associate them with or dissociate them from the namespace, respectively.

To select all the listed content classes, click in the checkbox at the top of the list. To deselect all the content classes after selecting all, click in the checkbox again.

3. Optionally, if the **Enable indexing** option is selected, select or deselect the **Enable indexing of custom metadata** option to enable or disable indexing of custom metadata, respectively.
4. If the **Enable indexing of custom metadata** option is enabled:
  - Optionally, select or deselect the **Enable full custom metadata indexing** option to enable or disable metadata query engine indexing of the full text of custom metadata, respectively.
  - Optionally, in the **Exclude Annotations from Indexing** field, specify the names of one or more annotations to be excluded from custom metadata indexing. Use a comma to separate each annotation name from the next.

Instead of explicit names, you can use patterns. The wildcard character for pattern matching is the asterisk (\*), which matches any number of characters of any type, including none. The asterisk can occur anywhere in the pattern.

Annotation names are case sensitive.

5. Click on the **Update Settings** button.

If you deselected the **Enable search** option, HCP displays a confirming message.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Update Settings** button.

## Reindexing an individual namespace

To reindex an individual namespace, in the **Search** panel for the namespace:

1. In the **Reindex** section of the **Search** panel:
  - In the first field, select either:
    - **Metadata Query Engine** to have the metadata query engine reindex the namespace
    - **HCP Search Facility** to have the HCP search facility reindex the namespace





---

**Tip:** The **Reindex** section displays either **Namespace indexed** or **Namespace not indexed** to indicate whether the namespace is currently included in the index for the selected search facility.

---

- Select either the **All objects** option or the **Objects modified after** option.

If you select the **Objects modified after** option, either type a date in the associated field or click on the calendar control (  ) to select a date. If you type a date, use this format: *mm/dd/yyyy*

If you enter an invalid date using the correct date format, HCP tries to convert it to a real date. For example, if you enter 11/31/2015, HCP converts it to 12/01/2015.

2. Click on the **Reindex Objects** button.

If you selected the **All objects** option, a confirming message appears.

In the window with the confirming message, select **I understand** to confirm that you understand the consequences of your action. Then click on the **Reindex Objects** button.



---

**Note:** If indexing is disabled for the namespace, the procedure above does not by itself start the reindexing process. To start reindexing the namespace, you need to reenale indexing. For information on doing that, see [“Setting search and indexing options”](#) above.

---

For more information on reindexing namespaces, see [“Content class and content property workflow”](#) on page 208. For information on reindexing namespaces from the namespace **Search** page, see [“Reindexing namespaces associated with a content class”](#) on page 233.



## Working with retention classes

Retention classes provide a means to consistently manage data that must remain in a namespace for a specific amount of time. For example, if local law requires that medical records be kept for a specified number of years, you can use a retention class to enforce that requirement.

Retention classes are defined on a per-namespace basis. The classes you create for one namespace are not visible in any other namespace.

You create retention classes in the Tenant Management Console. Users and applications can then use those classes as retention settings for objects.

This chapter describes retention classes and explains how to create, modify, and delete them.

For information on how users and applications use retention classes, see *Using a Namespace*.

## About retention classes

A **retention class** is a named value that, when used as the retention setting for an object, specifies how long the object must remain in its namespace. This value can be:

- An offset from the time the object is created. You specify an offset as numbers of years, months, and/or days.

For example, you could create a retention class named HlthReg-107 with an offset of 21 years. Then, all objects assigned HlthReg-107 as their retention setting could not be deleted for 21 years after they're created.

- One of these special values:
  - **Deletion Allowed** — The object can be deleted at any time.
  - **Deletion Prohibited** — The object can never be deleted by means of a normal delete operation. If the namespace is in enterprise mode, however, the object can be deleted by means of a privileged delete operation.
  - **Initial Unspecified** — The retention period for the object is unspecified. The object cannot be deleted by means of a normal delete operation while it has this retention setting. If the namespace is in enterprise mode, however, the object can be deleted by means of a privileged delete operation.

The retention period for an object assigned to a retention class is calculated from the value of that class. So, for example, if an object stored on October 8, 2011, is assigned to a retention class with an offset value of seven years, the retention period for that object expires on October 8, 2018.

You can choose to have HCP automatically delete the objects assigned to a retention class when they expire. This applies only to retention classes with a value that's an offset. It does not apply to retention classes with special values.

Automatic deletion of expired objects in retention classes occurs only if disposition is enabled. For information on disposition, see ["Disposition"](#) on page 25.

To view, create, and manage retention classes for a namespace, you use the **Retention Classes** panel for that namespace. To display this panel:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Compliance**.
4. On the left side of the **Compliance** panel, click on **Retention Classes**.




---

**Roles:** To view retention classes, you need the monitor, administrator, or compliance role. To create, modify, and delete retention classes, you need the compliance role.

---

## Understanding the retention class list

The **Retention Classes** panel lists the retention classes defined for a namespace. For each class, the list shows:

- The retention class name.
- Whether the retention class value is an offset or a special value.
- The retention class value.

A value that's an offset has this format:

$$A + ny + rm + nd$$

In this format, y is the number of years, m is the number of months, and d is the number of days. Only the measurement units with nonzero values are shown. For example, an offset of two years and 5 days looks like this:

$$A + 2y + 5d$$

- Whether expired objects in the retention class are automatically deleted (**Allow Disposition**).

To view the description of a listed retention class, click on the class name.

## Creating a retention class

To create a retention class in a given namespace, in the **Retention Classes** panel:

1. Click on **Create Retention Class**.
2. In the **Create Retention Class** panel:
  - In the **Retention Class Name** field, type a name for the retention class. Retention class names must be from one through 64 characters long, can contain only alphanumeric characters, hyphens (-), and underscores (\_), and are not case sensitive.
  - Do one of these:
    - To make the retention class value an offset, in the **Retention Method** field, select **Offset**. Then do one or more of:
      - In the **Years** field, type a number of years. Valid values are integers in the range zero through 9,999.
      - In the **Months** field, type a number of months. Possible values are integers in the range zero through 9,999.
      - In the **Days** field, type a number of days. Possible values are integers in the range zero through 9,999.
    - To make the retention class value a special value:
      1. In the **Retention Method** field, select **Special Value**.
      2. In the **Special Value** field, select the special value you want.
  - Optionally, in the **Description** field, type a description of the retention class. The description can be up to 1,024 characters long and can contain any valid UTF-8 characters, including white space.
  - Optionally, select the **Allow Disposition service to delete objects when expired** option to have HCP automatically delete expired objects in the retention class. This option is present only when the retention method is offset.
3. Click on the **Create Retention Class** button.

## Modifying a retention class

You can increase the value of a retention class at any time. These changes increase the value:

- From an offset to a larger offset
- From **Deletion Allowed** to an offset or **Deletion Prohibited**


If the namespace is in enterprise mode, you can decrease the value of a retention class at any time. These changes decrease the value:

- From an offset to a smaller offset
- From an offset to **Deletion Allowed**
- From **Deletion Prohibited** to an offset or **Deletion Allowed**

If the value of a retention class is **Initial Unspecified**, you can change it to any other value at any time. You can change the value to **Initial Unspecified** only from **Deletion Allowed**.

You can enable or disable the autodeletion feature at any time. You can also change the class description at any time.

To modify an existing retention class, in the **Retention Classes** panel:


1. In the list of retention classes, click on the edit control (  ) for the retention class you want to modify.
2. In the **Edit Retention Class** window, make the changes you want. For information on the fields and options in this panel, see ["Creating a retention class"](#) above.
3. Click on the **Update Settings** button.

## Deleting a retention class

You can delete a retention class only if the namespace in which the class is defined is in enterprise mode. You cannot delete a retention class in a namespace that's in compliance mode.

When you delete a retention class, the retention setting of each object in the class changes to **Deletion Prohibited**.

To delete a retention class, in the **Retention Classes** panel:

1. In the list of retention classes, click on the delete control (  ) for the retention class you want to delete.
2. In response to the confirming message, click on the **Delete Retention Class** button.

## Using privileged delete

Namespaces in enterprise mode support privileged delete operations. Users and applications with the applicable data access permissions can perform these operations through the HTTP namespace access protocol, the HCP Search Console, and HCP Data Migrator. If you have the compliance role through your HCP user account or group accounts, you can perform these operations through the Tenant Management Console.

This chapter describes the privileged delete feature and explains how to use the Tenant Management Console to perform privileged delete operations.

For information on performing privileged delete operations through:

- The HTTP protocol, see *Using a Namespace*.
- The Search Console, see *Searching Namespaces*
- HCP-DM, see *Using HCP Data Migrator*

## About privileged delete

Privileged delete is an HCP feature that enables you to delete objects even if they are under retention. This feature is available only for namespaces in enterprise mode. If a namespace is in compliance mode, you *cannot* delete objects that are under retention.

Privileged delete supports government regulations that require the destruction of certain types of data in response to changing circumstances. For example, companies may be required to destroy particular information about employees who leave. If that data is under retention, it cannot be deleted through normal delete operations.

If the namespace supports versioning, you can turn a privileged delete operation into a privileged purge operation. This deletes all versions of the target object.

When using privileged delete, you need to specify a reason for the deletion. The tenant log records all privileged delete operations, including the specified reasons, thereby creating an audit trail.

Using privileged delete, you can also delete objects that are not under retention. You would do this, for example, if you wanted to record the reason for an object deletion.

You cannot use privileged delete to delete objects that are on hold, regardless of their retention settings.



---

**Roles:** To perform a privileged delete operation through the Tenant Management Console, you need the compliance role.

---

## Object specification

With privileged delete, you can delete only one object at a time. To specify the object, you need to include the full path to it in its namespace (starting after `rest` or `data`). The path must begin with a forward slash (/).

For example, to delete the `Lee_Green_1254` object from the `Corporate/Employees` directory, you would specify:

```
/Corporate/Employees/Lee_Green_1254
```

Directory and object names are case sensitive. The separator is the forward slash (/).



Non-UTF-8 characters in directory and object names must be percent encoded. To avoid ambiguity, you should also percent-encode the characters listed in the table below.

Character	Percent-encoded value
Space	%20
Tab	%09
New line	%0A
Carriage return	%0D
+	%2B
%	%25
#	%23
?	%3F
&	%26

Percent-encoded values are not case sensitive.

## Performing a privileged delete

To use privileged delete to delete or purge an object:

1. In the top-level menu in the Tenant Management Console, click on **Namespaces**.
2. In the list of namespaces, click on the name of the namespace you want.
3. In the row of tabs below the namespace name, click on **Compliance**.
4. On the left side of the **Compliance** panel, click on **Privileged Delete**.



**Note:** This option is present only if the namespace is in enterprise mode and your user account includes the compliance role.

5. In the **Privileged Delete** panel:
  - In the **Object to Delete** field, type the path to and name of the object you want to delete. For information on identifying objects for deletion, see ["Object specification"](#) above.

- Optionally, select the **Purge all versions of this object** option to change the delete operation to a purge operation. This option appears only if versioning is enabled for the namespace.
  - In the **Reason for Deletion** field, type the reason why you're deleting the object. This text must be from one through 1,024 characters long and can contain any valid UTF-8 characters, including white space.
6. Click on the **Delete This Object** button.
  7. In response to the confirming message, click on the **Delete Object** button.

# Downloading HCP Data Migrator

HCP Data Migrator runs on both Windows and Unix clients. You download the applicable HCP-DM installation file from the Tenant Management Console. That file is then used to install HCP-DM on the client computers.

This chapter describes the system requirements for running HCP-DM and contains instructions for downloading the applicable installation file.

For an introduction to HCP-DM, see ["HCP Data Migrator"](#) on page 8. For information on installing and using HCP-DM, see *Using HCP Data Migrator*.

## HCP-DM system requirements

HCP-DM runs on any Windows or Unix client that supports the Oracle Java Runtime Environment (JRE) version 7 update 6 or later. The computer that runs HCP-DM must meet these minimum requirements:

- 1.6 Ghz processor
- 2 Gb RAM
- 100 Mbps Ethernet interface

Windows clients should have the most recent applicable Microsoft Windows Service Pack installed.

## Downloading the HCP-DM installation file

The HCP-DM installation file is:

- For Windows, either `hcpdm.exe` or `hcpdm.zip`
- For Unix, `hcpdm.tgz`




---

**Roles:** You can download an HCP-DM installation file while logged into the Tenant Management Console with any user account.

---

To download the HCP-DM installation file you want to use, in the Tenant Management Console:

1. In the top right corner of the Console window, mouse over the tools icon (  ) to open a dropdown menu.
2. In the dropdown menu, click on the option for the HCP-DM installation file you want:
  - **HCP-DM (Windows Installer)** for `hcpdm.exe`
  - **HCP-DM (zip)** for `hcpdm.zip`
  - **HCP-DM (tgz)** for `hcpdm.tgz`
3. Save the installation file in the location of your choice.









# Tenant Management Console alerts

The Tenant Management Console uses icons to report tenant and namespace status on the tenant **Overview**, **Namespaces**, and **Search** pages and on the namespace **Overview** panel. The Console also uses icons to report conflicting user accounts on the **Users** page. These icons, called **alerts**, are accompanied by text on the tenant **Overview** page and namespace **Overview** panel. On all pages on which they appear, alerts have text that's displayed when you mouse over them.








This appendix describes the alerts that can appear on the Console pages and shows the mouse-over text for each alert. Where applicable, the appendix also tells you how to respond to the alerts.

The alerts in each table in this appendix are listed alphabetically by their mouse-over text.





## Tenant Overview page alerts

Icon	Mouse-over text	Description
	Conflicting user accounts	Two or more user accounts have the same username. This can happen after an upgrade if, before the upgrade occurred, a user account and a data access account (created in an HCP release earlier than 5.0) had the same username. Resolve the conflict by merging or separating the conflicting accounts on the <b>Users</b> page in the Tenant Management Console.
	Irreparable and unavailable objects	One or more namespaces owned by the tenant contain irreparable objects, and one or more namespaces owned by the tenant contain unavailable objects. Please contact your HCP system administrator.  To see which objects are irreparable, go to the <b>Irreparable Objects</b> panel for the applicable namespaces. For information on this panel, see <a href="#">“Working with irreparable objects”</a> on page 175.
	Irreparable objects	One or more namespaces owned by the tenant contain irreparable objects. Please contact your HCP system administrator.  To see which objects are irreparable, go to the <b>Irreparable Objects</b> panel for the applicable namespaces. For information on this panel, see <a href="#">“Working with irreparable objects”</a> on page 175.
	Soft quota exceeded	The amount of storage used by all namespaces owned by the tenant exceeds the soft quota configured for the tenant. Consider deleting some objects from the namespaces or requesting an increase in the hard quota for the tenant.
	Tenant with DPL 1 namespaces that are not replicating	The tenant owns one or more namespaces that have a DPL of 1 (one) and are not being replicated. All HCP namespaces with a DPL of 1 should be replicated to ensure that the stored data is protected. If replication is not available, increase the DPL of the affected namespaces.  This alert appears only in HCP systems in which setting the DPL to one for a namespace can leave objects unprotected.
	Unavailable objects	One or more namespaces owned by the tenant contain unavailable objects. Please contact your HCP system administrator.




## Namespaces page alerts

Icon	Mouse-over text	Description
	AD single sign-on access disabled.	Active Directory single sign-on is currently not working with the HTTP protocol. Please contact your HCP system administrator.
	Anonymous access allowed	One or more enabled protocols allow clients to access the namespace without presenting user credentials for authentication.
	Appendable objects without CIFS/NFS	The namespace has appendable objects enabled, but neither the CIFS protocol nor the NFS protocol is enabled. Appendable objects work only with the CIFS and NFS protocols.
	Content classes but no custom metadata indexing	The namespace is associated with one or more content classes, but custom metadata indexing is disabled for the namespace. The metadata query engine is not indexing content properties for objects in the namespace.
	DPL 1 namespace is not replicating	<p>The namespace has a DPL of 1 (one) and is not being replicated. All HCP namespaces with a DPL of 1 should be replicated to ensure that the stored data is protected. If replication is not available, increase the namespace DPL.</p> <p>This alert appears only in HCP systems in which setting the DPL to one for a namespace can leave objects unprotected.</p>
	Hard quota exceeded	The amount of storage used by the namespace exceeds the hard quota configured for the namespace. Clients will not be able to add data to the namespace until either some existing objects are deleted or you increase the hard quota.
	Namespace <i>namespace-name</i> has <i>irreparable-object-count</i> irreparable objects	<p>The namespace contains the indicated number of irreparable objects. Please contact your HCP system administrator.</p> <p>To see which objects are irreparable, go to the <b>Irreparable Objects</b> panel for the namespace. For information on this panel, see <a href="#">“Working with irreparable objects”</a> on page 175.</p>

(Continued)







Icon	Mouse-over text	Description
	Namespace <i>namespace-name</i> has <i>irreparable-object-count</i> irreparable objects and <i>unavailable-object-count</i> unavailable objects	The namespace contains the indicated number of irreparable objects and the indicated number of unavailable objects. Please contact your HCP system administrator.  To see which objects are irreparable, go to the <b>Irreparable Objects</b> panel for the namespace. For information on this panel, see <a href="#">“Working with irreparable objects”</a> on page 175.
	Namespace <i>namespace-name</i> has <i>unavailable-object-count</i> unavailable objects	The namespace contains the indicated number of unavailable objects. Please contact your HCP system administrator.
	Soft quota exceeded	The amount of storage used by the namespace exceeds the soft quota configured for the namespace. Consider deleting some objects from the namespace or increasing its hard quota.
	Versioning without REST API	The namespace has versioning enabled, but the REST API is not enabled. Versioning works only with the REST API.

## Namespace Overview panel alerts


Icon	Mouse-over text	Description
	Anonymous access allowed	One or more enabled protocols allow clients to access the namespace without presenting user credentials for authentication.
	Appendable objects enabled without CIFS or NFS	The namespace has appendable objects enabled, but neither the CIFS protocol nor the NFS protocol is enabled. Appendable objects work only with the CIFS and NFS protocols.
	DPL 1 namespace is not replicating	The namespace has a DPL of 1 (one) and is not being replicated. All HCP namespaces with a DPL of 1 should be replicated to ensure that the stored data is protected. If replication is not available, increase the namespace DPL.  This alert appears only in HCP systems in which setting the DPL to one for a namespace can leave objects unprotected.




(Continued)

Icon	Mouse-over text	Description
	Hard quota exceeded	The amount of storage used by the namespace exceeds the hard quota configured for the namespace. Clients will not be able to add data to the namespace until either some existing objects are deleted or you increase the hard quota.
	Irreparable and unavailable objects	The namespace contains irreparable objects and unavailable objects. Please contact your HCP system administrator.  To see which objects are irreparable, go to the <b>Irreparable Objects</b> panel for the namespace. For information on this panel, see <a href="#">“Working with irreparable objects”</a> on page 175.
	Irreparable objects	The namespace contains irreparable objects. Please contact your HCP system administrator.  To see which objects are irreparable, go to the <b>Irreparable Objects</b> panel for the namespace. For information on this panel, see <a href="#">“Working with irreparable objects”</a> on page 175.
	Soft quota exceeded	The amount of storage used by the namespace exceeds the soft quota configured for the namespace. Consider deleting some objects from the namespace or increasing its hard quota.
	Unavailable objects	The namespace contains unavailable objects. Please contact your HCP system administrator.
	Versioning enabled without REST API	The namespace has versioning enabled, but the REST API is not enabled. Versioning works only with the REST API.

## Search page alert

Icon	Mouse-over text	Description
	Namespaces without custom metadata indexing	The content class is associated with one or more namespaces for which custom metadata indexing is disabled. The metadata query engine is not indexing content properties for objects in those namespace.

## Users page alert

Icon	Mouse-over text	Description
	Conflicting user accounts	Another user account has the same username as this account. Resolve the conflict by merging or separating the conflicting accounts.

## Tenant log messages

The tenant log contains messages about events that happen at the tenant and namespace levels. The table in this appendix lists the messages HCP can write to the tenant log. The messages are listed in order by event ID.

For each message, the table shows:

- The message ID
- The short form of the message, which identifies the event to which the message applies
- An explanation of the message
- The action, if any, you should take in response to the message
- The message severity

For more information on the system log, see [“Monitoring the tenant”](#) on page 108.

ID	Event	Explanation	Action	Severity
2005	HCP found an unavailable object	HCP could not repair an object because the object was unavailable.	Contact your HCP system administrator.	Warning
2006	HCP found an irreparable object	HCP found a broken object it could not repair.	Contact your HCP system administrator.	Error
2028	HCP found an irreparable object	HCP was unable to repair the object. The repair may be retried at a later time.	Contact your HCP system administrator.	Error
2044	HCP found an unavailable object	HCP could not repair an object because the object was unavailable.	Contact your HCP system administrator.	Warning
2046	HCP found an irreparable object	HCP found a broken object it could not repair.	Contact your HCP system administrator.	Error
2070	Object has been shredded	An object was shredded.	No action is required.	Notice
2087	Disposition service stopped: run complete	The disposition service finished successfully.	No action is required.	Notice
2088	Disposition service stopped without finishing	The disposition service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2089	Disposition service stopped: run complete	The disposition service finished successfully.	No action is required.	Notice
2090	Disposition service stopped without finishing	The disposition service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Warning
2092	Disposition service stopped without finishing	The disposition service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2093	Disposition service stopped without finishing	The disposition service stopped without completing its run. The service will resume at some point in the future.	No action is required.	Notice
2154	Additional namespaces included in tenant replication	The indicated namespaces were selected to be included in replication of the tenant.	No action is required.	Notice

(Continued)

ID	Event	Explanation	Action	Severity
2155	One or more namespaces removed from tenant replication	The indicated namespaces were removed from replication of the tenant.	No action is required.	Notice
2156	Replication automatically paused for this tenant	Replication of the tenant was automatically paused for the indicated reason.	If the cause is one or more namespace name collisions, rename each indicated namespace. If the cause is that the replica does not support the DPL of one or more namespaces, lower the DPL of each indicated namespace. Alternatively, in either case, you can deselect the namespace from being replicated. After you make the necessary changes, notify your HCP system administrator that the problem has been resolved.	Error
2157	Namespace replication collision detected	A namespace replication collision was detected, possibly requiring intervention from the tenant administrator.	If the cause is one or more namespace name collisions, rename each indicated namespace. If the cause is that the replica does not support the DPL of one or more namespaces, lower the DPL of each indicated namespace. Alternatively, in either case, you can deselect the namespace from being replicated. After you make the necessary changes, notify your HCP system administrator that the problem has been resolved.	Notice

(Continued)

ID	Event	Explanation	Action	Severity
2160	User account replicated with collisions	Either or both of two user accounts with the same user ID on a 4.x system were modified on that system, resulting in conflicting values for one or more properties. On replication to this system, the values for those properties were taken from the account with roles.	Ensure that the user account is configured correctly.	Warning
2351	Group account created	A user created a group account.	No action is required.	Notice
2353	Group account updated	A user updated a group account.	No action is required.	Notice
2355	Group account deleted	A user deleted a group account.	No action is required.	Notice
2613	HCP search facility index recovery started for namespace	A user reset HCP search facility indexing for a namespace.	If indexing was disabled for the namespace, reenable it to start rebuilding the HCP search facility index. (This also reenables metadata query engine indexing.)	Warning
2900	Privileged delete requested	A user requested a privileged delete operation.	No action is required.	Notice
2901	Privileged delete succeeded	A privileged delete operation succeeded.	No action is required.	Notice
2902	Privileged delete failed	A privileged delete operation failed.	No action is required.	Notice
2903	Retention class created	A user created a retention class.	No action is required.	Notice
2904	Retention class updated	A user updated a retention class.	No action is required.	Notice
2905	Retention class deleted	A user deleted a retention class.	No action is required.	Notice
2906	Retention mode set	The namespace retention mode has been changed.	No action is required.	Notice
2907	Privileged purge requested	A user requested a privileged purge operation.	No action is required.	Notice

(Continued)

ID	Event	Explanation	Action	Severity
2908	Privileged purge succeeded	A privileged purge operation succeeded.	No action is required.	Notice
2909	Privileged purge failed	A privileged purge operation failed.	No action is required.	Notice
3004	Namespace created	A user created a namespace.	No action is required.	Notice
3005	Namespace updated	A user updated a namespace.	No action is required.	Notice
3006	Namespace deleted	A user deleted a namespace.	No action is required.	Notice
3011	User account created	A user created a user account.	No action is required.	Notice
3012	User account updated	A user updated a user account.	No action is required.	Notice
3013	User account deleted	A user deleted a user account.	No action is required.	Notice
3014	User account is disabled	A user tried to log in with a disabled user account.	Reenable the user account to allow the user to log in.	Warning
3015	User account disabled	A user account has been disabled.	No action is required.	Notice
3016	User account enabled	A user account has been enabled.	No action is required.	Notice
3017	User account password changed	A user changed the password for a user account.	No action is required.	Notice
3018	User account failed login	A user tried to log in with a username and password that are not valid for any user account.	Have the user log in with a username and password that are valid for a user account.	Warning
3019	Failed login to the Search Console	A user tried to log into the Search Console with a username and password that are not valid for any user account.	Have the user log into the Search Console with a username and password for that are valid for a user account.	Warning
3020	Namespace over hard quota	The amount of storage used by the namespace exceeds the configured hard quota.	Delete some objects from the namespace or increase the hard quota.	Warning

(Continued)

ID	Event	Explanation	Action	Severity
3021	Namespace under hard quota	The amount of storage used by the namespace is under the configured hard quota	No action is required.	Warning
3022	Namespace over soft quota	The amount of storage used by the namespace exceeds the configured soft quota.	Consider deleting some objects from the namespace or increasing the hard quota for the namespace.	Warning
3023	Namespace under soft quota	The amount of storage used by the namespace is under the configured soft quota.	No action is required.	Warning
3024	Tenant over soft quota	The amount of storage used by all namespaces owned by the tenant exceeds the soft quota configured for the tenant.	Consider deleting some objects from the namespaces or requesting an increase in the hard quota for the tenant.	Warning
3025	Tenant under soft quota	The amount of storage used by all namespaces owned by the tenant is under the soft quota configured for the tenant.	No action is required.	Warning
3028	Failed user account login attempt	An attempt to log into a tenant failed because the user account could not be authenticated.	No action is required.	Warning
3032	Tenant at namespace quota	The number of namespaces is equal to the maximum allowed for this tenant.	No action is required.	Warning
3033	Tenant over namespace quota	The number of namespaces is greater than the maximum allowed for this tenant.	Either delete one or more namespaces or have your HCP system administrator increase the namespace quota.	Warning
3037	Username conflict	Multiple user accounts have the same username. All user accounts must have a unique username.	Rename one account or merge duplicate accounts together.	Warning
3508	HCP found an irreparable object	HCP found a broken object it could not repair.	Contact your HCP system administrator.	Error
3998	Search enabled or disabled	A user enabled or disabled search.	No action is required.	Notice



(Continued)

ID	Event	Explanation	Action	Severity
3999	Search indexing enabled or disabled	A user enabled or disabled search indexing.	No action is required.	Notice
4000	HCP search facility indexing failure	The HCP search facility encountered an object it could not index.	Contact your HCP system administrator.	Error
4002	User account created	A user created a user account.	No action is required.	Notice
4003	User account updated	A user updated a user account.	No action is required.	Notice
4004	User account deleted	A user deleted a user account.	No action is required.	Notice
4005	User authenticated	A user login to the Tenant Management Console was successfully authenticated.	No action is required.	Notice
4006	Authentication attempt by unknown user	A user tried to log in with an unknown username.	Have the user log in with a valid username and password.	Warning
4007	Account reenabled by timer	A disabled security user account has been automatically reenabled.	No action is required.	Notice
4008	Account is disabled	A user tried to log in with a disabled account.	Reenable the user account to allow the user to log in.	Warning
4009	Account has been inactive for too long	A user tried to log in with an account that was disabled due to inactivity.	Reenable the user account to allow the user to log in.	Warning
4010	Account does not include the required roles	A user tried to log in with an account that does not include a required role.	Update the account to include the required role to allow the user to log in.	Warning
4011	Password is invalid	A user tried to log in with an invalid password.	Have the user log in with a valid username and password.	Warning
4012	Remote authentication server error	The login for a remotely authenticated user failed due to an error communicating with a RADIUS server.	Contact your HCP system administrator.	Warning
4013	Password changed	A user changed the password for a user account.	No action is required.	Notice

(Continued)

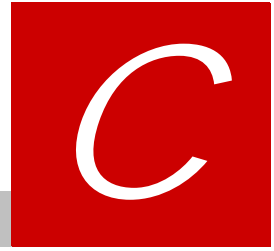
ID	Event	Explanation	Action	Severity
4014	Account enabled	A user account has been enabled.	No action is required.	Notice
4015	Account disabled	A user account has been disabled.	No action is required.	Notice
4016	Account disabled due to too many failed logins	A user account has been automatically disabled due to too many failed login attempts.	Reenable the user account and have the user log in with a valid username and password.	Warning
4017	Account will be reenabled	A security user account will be reenabled automatically after a waiting period.	No action is required.	Notice
4018	User authenticated	A user login to the Search Console was successfully authenticated.	No action is required.	Notice
4019	Configuration changed	A user changed a configuration value of an HCP component.	No action is required.	Notice
4020	Configuration changed	A user changed a configuration value of an HCP component.	No action is required.	Notice
4021	Irreparable object acknowledged	A user acknowledged an irreparable object.	No action is required.	Warning
4022	All irreparable objects acknowledged	A user acknowledged all irreparable objects.	No action is required.	Warning
4023	Unauthorized action	A user has requested an operation that is not authorized for the user account.	If the user should be allowed to perform this operation, add the required role to the user account.	Warning
4024	User account created	A user created a user account.	No action is required.	Notice
4025	User account updated	A user updated a user account.	No action is required.	Notice
4026	User account deleted	A user deleted a user account.	No action is required.	Notice
4027	User account is disabled	A user tried to log in with a disabled user account.	Reenable the user account to allow the user to log in.	Warning

(Continued)

ID	Event	Explanation	Action	Severity
4028	User account disabled due to too many failed logins	A user account has been automatically disabled due to too many failed login attempts.	Reenable the user account to allow the account user to log in.	Warning
4029	User account disabled	A user account has been disabled.	No action is required.	Notice
4030	User account password changed	A user changed the password for a user account.	No action is required.	Notice
4031	User accounts merged	A user merged multiple user accounts with the same username into a single account.	No action is required.	Notice
4100	Object replicated with collisions	An object being replicated conflicts with an existing object on the target system. The object has been stored in the .lost+found directory on the target system.	No action is required.	Warning
4101	Object did not replicate	An object was not replicated.	Contact your HCP system administrator.	Error
4102	Object did not replicate; will retry later	An object was not replicated. Replication of the object will be retried later.	Monitor the replica to see whether this object is eventually replicated. If the object does not replicate within one week, contact your HCP system administrator.	Warning
4114	Metadata query engine indexing failure	The metadata query engine encountered an object it could not index.	If this situation persists, contact your HCP system administrator.	Warning
4115	Metadata query engine checkpoint reset	A user reset the metadata query engine checkpoint for the indicated namespace.	No action is required.	Warning
4122	Failure adding namespace to the search index.	The HCP search facility could not create the index for a namespace because the system limit was reached.	No action is required. If this situation persists, contact your authorized service provider.	Warning
4123	Namespace was successfully added to index	Namespace was added to the index	No action is required.	Notice

(Continued)

ID	Event	Explanation	Action	Severity
4124	Content class created	A user created a content class.	No action is required.	Notice
4125	Content class updated	A user updated a content class.	No action is required.	Notice
4126	Content class deleted	A user deleted a content class.	No action is required.	Notice
4127	Namespaces associated with content class	A user associated namespaces with a content class.	No action is required.	Notice
4128	Content classes associated with namespace	A user associated content classes with a namespace.	No action is required.	Notice
4220	Namespace tags updated	A user updated the tags for a namespace.	No action is required.	Notice
4225	Namespace default settings updated	A user updated the namespace default settings.	No action is required.	Notice



# Browser configuration for single sign-on with Active Directory

If a tenant is configured to support AD authentication, you can use a recognized AD user account to access the Tenant Management Console with single sign-on. However, for this to work, the web browser you use to access the Console must be configured to support single sign-on.

This appendix contains instructions for configuring Windows Internet Explorer® and Mozilla® Firefox® to support single sign-on.

## Configuring Windows Internet Explorer for single sign-on

To configure Windows Internet Explorer for single sign-on with Active Directory:

1. Open Internet Explorer.
2. On the **Tools** menu, click on **Internet Options**.
3. In the **Internet Options** window, click on the **Security** tab.
4. On the **Security** page, select **Local intranet**.
5. Click on the **Sites** button.
6. In the **Local intranet** window, ensure that all the options are selected.
7. Click on the **Advanced** button.
8. In the **Add this website to the zone** field, do either of these:
  - To enable single sign-on with HTTP, type:  
  
`http://*.hcp-name.domain-name`  
  
For example:  
  
`http://*.hcp.example.com`
  - To enable single sign-on with HTTPS, type:  
  
`https://*.hcp-name.domain-name`  
  
For example:  
  
`https://*.hcp.example.com`
9. Click on the **Add** button.
10. Click on the **Close** button.
11. In the **Local intranet** window, click on the **OK** button.
12. In the **Internet Options** window, click on the **Advanced** tab.

13. In the **Settings** list, under **Security**, select **Enable Integrated Windows Authentication**.
14. Click on the **OK** button.
15. Close Internet Explorer.

## Configuring Mozilla Firefox for single sign-on

To configure Mozilla Firefox for single sign-on with Active Directory:

1. Open Firefox.
2. In the address field in the Firefox window, enter:  
  
about:config
3. In response to the warning message, click on the **I'll be careful, I promise!** button.
4. In the **Preference Name** list, double-click on **network.negotiate-auth.delegation-uris**.
5. In the **Enter string value** window, type:

*http://\*.hcp-name.domain-name,https://\*.hcp-name.domain-name*

For example:

*http://\*.hcp.example.com,https://\*.hcp.example.com*

6. Click on the **OK** button.
7. In the **Preference Name** list, double-click on **network.negotiate-auth.trusted-uris**.
8. In the **Enter string value** window, type:

*http://\*.hcp-name.domain-name,https://\*.hcp-name.domain-name*

9. Click on the **OK** button.
10. Close Firefox.







# Glossary

## A

### **access control entry (ACE)**

In an access control list, a grant of permissions to perform various operations on an object. Each access control entry grants permissions to a specific user or group of users.

### **access control list (ACL)**

Optional metadata consisting of a set of grants of permissions to perform various operations on an object. Permissions can be granted to individual users or to groups of users.

ACLs are provided by users or applications and are specified as either XML or JSON.

### **access protocol**

See [namespace access protocol](#).

### **ACE**

See [access control entry \(ACE\)](#).

### **ACL**

See [access control list \(ACL\)](#).

### **Active Directory (AD)**

A Microsoft product that, among other features, provides user authentication services.

### **Active Directory domain**

A structural unit within Active Directory that serves as a container for objects such as users and groups.

## **Active Directory forest**

A structural unit within Active Directory that contains collections of Active Directory domains.

## **AD**

See [Active Directory \(AD\)](#).

## **alert**

A graphic that indicates the status of some particular element of an HCP system in the Tenant Management Console.

## **allow list**

A list of IP addresses that are allowed access to the HCP system when using a particular external interface (such as the HTTP protocol).

## **annotation**

A discrete unit of custom metadata. Annotations are typically specified in XML format.

## **anonymous access**

A method of access to a namespace wherein the user or application gains access without presenting any credentials. *See also* [authenticated access](#).

## **appendable object**

An object to which data can be added after it has been successfully stored. Appending data to an object does not modify the original fixed-content data, nor does it create a new version of the object. Once the new data is added to the object, that data also cannot be modified.

Appendable objects are supported only with the CIFS and NFS protocols.

## **atime**

In POSIX file systems, metadata that specifies the date and time a file was last accessed. In HCP, POSIX metadata that initially specifies the date and time at which an object was ingested. HCP does not automatically change the **atime** value when the object is accessed.

Users and applications can change this metadata, thereby causing it to no longer reflect the actual storage time. Additionally, HCP can be configured to synchronize **atime** values with retention settings.

**authenticated access**

A method of access to the HCP system or a namespace wherein the user or application presents credentials to gain access. *See also* [anonymous access](#).

**authentication**

*See* [user authentication](#).

**B****bucket**

The HS3 term for a namespace.

**C****chargeback report**

A report that contains historical statistics about tenant or namespace capacity and bandwidth usage, broken out either by hour or by day.

**CIFS**

Common Internet File System. One of the namespace access protocols supported by HCP. CIFS lets Windows clients access files on a remote computer as if the files were part of the local file system.

**comma-separated-values (CSV) file**

A text file containing tabular data. Each line in a CSV file corresponds to a table row and contains a set of comma-separated values, each of which corresponds to a table column.

**compliance mode**

The retention mode in which objects under retention cannot be deleted through any mechanism. This is the more restrictive retention mode.

**content class**

A content class is a named construct that is used to characterize objects in one or more namespaces. Content classes use object metadata to impose structure on the unstructured namespace content. They do this through content properties.

### **content property**

A content property is a named construct used to extract an element or attribute value from custom metadata that's well-formed XML. Content properties use XPath expressions to identify the metadata of interest.

### **cryptographic hash value**

A system-generated metadata value calculated by a cryptographic hash algorithm from object data. This value is used to verify that the content of an object has not changed.

### **CSV file**

See [comma-separated-values \(CSV\) file](#).

### **custom metadata**

User-supplied information about an HCP object. Custom metadata is specified as one or more annotations, where each annotation is a discrete unit of information about the object. Users and applications can use custom metadata to understand and repurpose object content.

## **D**

### **data access permission mask**

A set of permissions that determine which of these operations are allowed in a namespace: read (including read ACL), write (including write ACL and change owner), delete, purge, privileged operations, and search. Data access permission masks are defined at the system, tenant, and namespace level. The effective permissions for a namespace are those that are allowed at all three levels.

### **Data Migrator**

See [HCP Data Migrator \(HCP-DM\)](#).

### **data protection level (DPL)**

The number of copies of the data for an object HCP must maintain in the repository. The DPL for an object is determined by the service plan that applies to the namespace containing the object.

### **dead properties**

For WebDAV only, arbitrary name/value pairs that the server stores but does not use or modify in any way.

**deny list**

A list of IP addresses that are denied access to the HCP system when using a particular external interface (such as the HTTP protocol).

**disposition**

The automatic deletion of an expired object by HCP.

**DNS**

See [domain name system \(DNS\)](#).

**domain**

A group of computers and devices on a network that are administered as a unit.

**domain name system (DNS)**

A network service that resolves domain names into IP addresses for client access.

**DPL**

See [data protection level \(DPL\)](#).

**dynamic DPL**

A namespace data protection level that, at any given time, matches the system-level DPL setting.

**E**

See [HCP S Series Node](#).

**enterprise mode**

The retention mode in which these operations are allowed:

- Privileged delete
- Changing the retention class of an object to one with a shorter duration
- Reducing retention class duration
- Deleting retention classes

This is the less restrictive retention mode.

**expired object**

An object that is no longer under retention.

**F****fixed-content data**

A digital asset ingested into HCP and preserved in its original form as the core part of an object. Once stored, fixed-content data cannot be modified.

**G****GID**

POSIX group identifier.

**group account**

A representation of an Active Directory group in HCP. A group account enables Active Directory users in the Active Directory group to access one or more HCP interfaces.

**H****hard quota**

For a tenant, the total amount of storage available to the tenant for allocation to its namespaces. For a namespace, the total amount of storage available for storing objects in the namespace.

**hash value**

See [cryptographic hash value](#).

**HCP**

See [Hitachi Content Platform \(HCP\)](#).

**HCP Data Migrator (HCP-DM)**

An HCP utility that can transfer data from one location to another, delete data from a location, and change object metadata in a namespace. Each location can be a local file system, an HCP namespace, a default namespace, or an HCAP 2.x archive.

**HCP-DM**

See [HCP Data Migrator \(HCP-DM\)](#).

**HCP-FS**

See [HCP file system \(HCP-FS\)](#).

**HCP file system (HCP-FS)**

The HCP runtime component that represents each object in a namespace as a set of files. One of these files contains the object data. The others contain the object metadata.

**HCP management API**

A RESTful HTTP interface to a subset of the administrative functions of an HCP system. Using this API, you can manage tenants, namespaces, content classes, retention classes, and tenant-level user and group accounts.

**HCP metadata query API**

See [metadata query API](#).

**HCP namespace**

A namespace that supports user authentication for data access through the HTTP, HS3, and CIFS protocols. HCP namespaces also support storage usage quotas, access control lists, and versioning. An HCP system can have multiple HCP namespaces.

**HCP service**

See [service](#).

**HDDS**

See [Hitachi Data Discovery Suite \(HDDS\)](#).

**HDDS search facility**

One of the search facilities available for use with the HCP Search Console. This facility interacts with Hitachi Data Discovery Suite.

## **Hitachi Content Platform (HCP)**

A distributed object-based storage system designed to support large, growing repositories of fixed-content data. HCP provides a single scalable environment that can be used for archiving, business continuity, content depots, disaster recovery, e-discovery, and other services. With its support for multitenancy, HCP securely segregates data among various constituents in a shared infrastructure. Clients can use a variety of industry-standard protocols and various HCP-specific interfaces to access and manipulate objects in an HCP repository.

## **Hitachi Data Discovery Suite (HDDS)**

A Hitachi product that enables federated searches across multiple HCP systems and other supported systems.

## **hold**

A condition that prevents an object from being deleted by any means and from having its metadata modified, regardless of its retention setting, until it is explicitly released.

## **HS3 API**

One of the namespace access protocols supported by HCP. HS3 is a RESTful, HTTP-based API that is compatible with Amazon S3. Using HS3, users and applications can create and manage buckets and bucket contents.

## **HSwift API**

One of the namespace access protocols supported by HCP. HSwift is a RESTful, HTTP-based API that is compatible with OpenStack Swift. Using HSwift, users and applications can create and manage containers and container contents.

## **HTTP**

HyperText Transfer Protocol. One of the namespace access protocols supported by HCP. In the context of namespace access, the HTTP protocol is also called the REST API.

HCP also uses HTTP for client communication with the Tenant Management and Search Consoles, for client access through the HCP management API, and for access to namespace content through the metadata query API.

## **HTTPS**

HTTP with SSL security. See [HTTP](#) and [SSL](#).



## I

### **index**

An index of the objects in namespaces that is used to support search operations. Each of the two search facilities, the metadata query engine and the HDDS search facility, creates and maintains its own separate index.

### **index setting**

The property of an object that determines whether the metadata query engine indexes the custom metadata associated with the object.

### **Integrated Windows authentication**

A Microsoft authentication mechanism that enables clients to authenticate to a web server by using the Windows user information currently cached on the client computer, thereby removing the need to explicitly log in.

## J

### **JSON**

JavaScript Object Notation. A language-independent format for encoding data in the form of name/value pairs.

## L

### **local authentication**

Authentication wherein HCP internally checks the validity of the specified username and password.

## M

### **management API**

See [HCP management API](#).

### **metadata**

System-generated and user-supplied information about an object. Metadata is stored as an integral part of the object it describes, thereby making the object self-describing.

### **metadata query API**

A RESTful HTTP interface that lets you search HCP for objects that meet specified metadata-based or operation-based criteria. With this API, you can search not only for objects currently in the repository but also for information about objects that are no longer in the repository.

### **metadata query engine**

One of the search facilities available for use with HCP. The metadata query engine works internally to perform searches and return results either through the metadata query API or to the HCP Metadata Query Engine Console (also known as the HCP Search Console).

### **Metadata Query Engine Console**

The web application that provides interactive access to the HCP search functionality provided by the metadata query engine.

## **N**

### **namespace**

A logical partition of the objects stored in an HCP system. A namespace consists of a grouping of objects such that the objects in one namespace are not visible in any other namespace. Namespaces are configured independently of each other and, therefore, can have different properties.

### **namespace access protocol**

A protocol that can be used to transfer data to and from namespaces in an HCP system. HCP supports the HTTP, HS3, WebDAV, CIFS, NFS, and SMTP protocols for access to HCP namespaces.

### **namespace quota**

The number of namespaces HCP reserves for an HCP tenant out of the total number of namespaces the system can have.

## **NFS**

Network File System. One of the namespace access protocols supported by HCP. NFS lets clients access files on a remote computer as if the files were part of the local file system.

## O

### **object**

An exact digital representation of data as it existed before it was ingested into HCP, together with the system and custom metadata that describes that data. Objects can also include ACLs that give users and groups permission to perform certain operations on the object.

An object is handled as a single unit by all transactions and internal processes, including shredding, indexing, versioning, and replication.

### **object-based query**

In the metadata query API, a query that searches for objects based on object metadata. This includes both system metadata and the content of custom metadata and ACLs. The query criteria can also include the object location (that is, the namespace and/or directory that contains the object).

Object-based queries search only for objects that currently exist in the repository. For objects with multiple versions, object-based queries return only the current version.

### **operation-based query**

In the metadata query API, a query that searches not only for objects currently in the repository but also for information about objects that have been deleted by a user or application, deleted through disposition, purged, or pruned. For namespaces that support versioning, operation-based queries can return both current and old versions of objects.

Criteria for operation-based queries can include object status (for example, created or deleted), change time, index setting, and location (that is, the namespace and/or directory that contains the object).

## P

### **permission**

One of these:

- In a data access permission mask, the condition of allowing a specific type of operation to be performed in a namespace.
- In a user account, the granted ability to perform a specific type of operation in a given namespace.

- In an ACL associated with an object, the granted ability to perform a specific type of operation on the object.
- The granted ability to access the HCP Tenant Management Console and to perform a specific activity or set of activities in that Console. Permissions of this type are granted by roles associated with the user account.

### **permission mask**

See [data access permission mask](#).

### **policy**

One or more settings that influence how transactions and internal processes work on objects. Such a setting can be a property of an object, such as retention, or a property of a namespace, such as versioning.

### **POSIX**

Portable Operating System Interface for UNIX. A set of standards that define an application programming interface (API) for software designed to run under heterogeneous operating systems. HCP-FS is a POSIX-compliant file system, with minor variations.

### **privileged delete**

A delete operation that works on an object regardless of whether the object is under retention, except if the object is on hold. This operation is available only to users and applications with explicit permission to perform it.

Privileged delete operations work only in namespaces in enterprise mode.

### **privileged purge**

A purge operation that works on an object regardless of whether the object is under retention, except if the object is on hold. This operation is available only to users and applications with explicit permission to perform it.

Privileged purge operations work only in namespaces in enterprise mode.

### **protocol**

See [namespace access protocol](#).

**pruning**

See [version pruning](#).

**purge**

The operation that deletes all versions of an object.

**Q****query**

A request submitted to HCP to return metadata for objects that satisfy a specified set of criteria. Also, to submit such a request.

**query API**

See [metadata query API](#).

**R****RADIUS**

Remote Authentication Dial-In User Service. A protocol for authenticating credentials that authorize access to an IP network.

**recognized Active Directory user account**

An Active Directory user account for a user that belongs to one or more Active Directory groups for which corresponding group accounts are defined in HCP.

**remote authentication**

Authentication wherein HCP uses a remote service to check the validity of the specified username and password.

**replica**

The HCP system to which the replication service copies objects and other information from the primary system during normal replication.

**replication**

The process of keeping selected tenants and namespaces in two HCP systems in sync with each other. Basically, this entails copying object creations, deletions, and metadata changes from each system to the other or from one system to the other. HCP also replicates tenant and

namespace configuration, user and group accounts, retention classes, content classes, all compliance log messages, and all HCP tenant log messages.

### **repository**

The aggregate of the namespaces defined for an HCP system.

### **REST**

Representational State Transfer. A software architectural style that defines a set of rules (called constraints) for client/server communication. In a REST architecture:

- Resources (where a resource can be any coherent and meaningful concept) must be uniquely addressable.
- Representations of resources (for example, in XML format) are transferred between clients and servers. Each representation communicates the current or intended state of a resource.
- Clients communicate with servers through a uniform interface (that is, a set of methods that resources respond to) such as HTTP.

### **REST API**

One of the namespace access protocols supported by HCP. The REST API is also called the HTTP protocol.

### **retention class**

A named retention setting. The value of a retention class can be a duration, Deletion Allowed, Deletion Prohibited, or Initial Unspecified.

### **retention hold**

See [hold](#).

### **retention mode**

A namespace property that affects which operations are allowed on objects under retention. A namespace can be in either of two retention modes: compliance or enterprise.

### **retention period**

The period of time during which an object cannot be deleted (except by means of a privileged delete).

**retention setting**

The property that determines the retention period for an object.

**role**

A named collection of permissions that can be associated with an HCP user account, where each permission allows the user to perform some specific interaction or set of interactions with the HCP Tenant Management Console and management API. Roles generally correspond to job functions.

**S****Search Console**

The web application that provides interactive access to HCP search functionality. When the Search Console uses the HCP metadata query engine for search functionality, it is called the Metadata Query Engine Console.

**search facility**

An interface between the HCP Search Console and the search functionality provided by the metadata query engine or HDDS. Only one search facility can be selected for use with the Search Console at any given time.

**service**

A background process that performs a specific function that contributes to the continuous tuning of the HCP system. In particular, services are responsible for optimizing the use of system resources and maintaining the integrity and availability of the data stored in the HCP repository.

**service plan**

A named option that can be associated with a namespace and that determines how HCP manages the objects in that namespace. Service plan names are system specific.

**shred setting**

The property that determines whether an object will be shredded or simply removed when it's deleted from HCP.

**shredding**

The process of deleting an object and overwriting the locations where all its copies were stored in such a way that none of its data or metadata can be reconstructed. Also called **secure deletion**.

### **single sign-on**

In a Windows environment, the use of an already authenticated Active Directory user account to access the Tenant Management Console, HCP Search Console, or Namespace Browser without the need to explicitly log in.

### **SMTP**

Simple Mail Transfer Protocol. The namespace access protocol HCP uses to receive and store email data directly from email servers.

### **SNMP**

Simple Network Management Protocol. A protocol HCP uses to facilitate monitoring and management of the system through an external interface.

### **soft quota**

The percentage point at which HCP notifies a tenant that allocated storage space is being used up. For a tenant, the soft quota measures the space used in all the namespaces the tenant owns relative to the hard quota for that tenant. For a namespace, the soft quota measures the space used in only that namespace relative to the hard quota for that namespace.

### **SSL**

Secure Sockets Layer. A key-based Internet protocol for transmitting documents through an encrypted link.

### **syslog**

A protocol used for forwarding log messages in an IP network. HCP uses syslog to facilitate system monitoring through an external interface.

### **System Management Console**

The system-specific web application that lets you monitor and manage HCP.

### **system metadata**

System-managed properties that describe the content of an object. System metadata includes policies, such as retention and data protection level, that influence how transactions and services affect the object.



**systemwide permission mask**

The data access permission mask defined at the HCP system level. The systemwide permission mask applies across all tenants and namespaces.

**T****tag**

An arbitrary text string associated with an HCP namespace. Tags can be used to group namespaces and to filter namespace lists.

**tenant**

An administrative entity created for the purpose of owning and managing namespaces. Tenants typically correspond to customers or business units.

**Tenant Management Console**

The tenant-specific web application that lets you monitor and manage tenants and namespaces.

**U****UID**

POSIX user ID.

**Unix**

Any UNIX-like operating system (such as UNIX itself or Linux).

**user account**

A set of credentials that gives a user access to one or more of the Tenant Management Console, the HCP management API, the HCP Search Console, namespace content through the namespace access protocols, the metadata query API, and HCP Data Migrator.

**user authentication**

The process of checking that the combination of a specified username and password is valid when a user tries to log into the Tenant Management Console or the HCP Search Console, to access the HCP system through the management API, or to access a namespace.

## V

### **versioning**

An optional namespace feature that enables the creation and management of multiple versions of an object.

### **version pruning**

The automatic deletion of previous versions of objects that are older than a specified amount of time.

## W

### **WebDAV**

Web-based Distributed Authoring and Versioning. One of the namespace access protocols supported by HCP. WebDAV is an extension of HTTP.

### **Windows workgroup**

A named collection of computers on a LAN that share resources such as printers and file servers.

### **workgroup**

See [Windows workgroup](#).

### **WORM**

Write once, read many. A data storage property that protects the stored data from being modified or overwritten.

## X

### **XML**

Extensible Markup Language. A standard for describing data content using structural tags called elements.

### **XPath**

A language used to formulate expressions that navigate through and select elements and attributes in XML documents.

# Index

## Symbols

[internal] event initiator 111  
[remote admin] event initiator 111  
[service] event initiator 111

## A

access control entries 30–31  
access control list collisions 41–42  
access control lists  
    See [ACLs](#)  
access to Tenant Management Console 48  
acknowledging irreparable objects 176–177  
ACLs  
    about 2–3, 30–31  
    changing enforcement of 161  
    collisions 41–42  
    enabling use of 160–161  
    enforcing 31  
    use of 31  
ACLs panel 161  
Active Directory  
    authentication 72–73  
    with CIFS 192  
    single sign-on 48, 72  
    single sign-on option for HS3 189  
    single sign-on option for HTTP 189  
    user permissions 48  
Active Directory groups  
    See [groups, Active Directory](#)  
Active Directory user accounts  
    See [user accounts, Active Directory](#)  
adding  
    See also [creating](#)  
    content properties to content  
        classes 228–229  
    content properties to content classes  
        individually 229  
    email recipients 120–121  
    IP addresses to Allow/Deny lists 182

administrative user accounts  
    See [roles](#)  
administrator role 64  
alerts  
    content classes 257  
    namespaces 136, 142, 255–257  
    Namespaces page 255–256  
    Overview page, tenant 254  
    Overview panel, namespace 256–257  
    tenant 98, 254  
    user accounts 258  
    Users page 258  
All Events panel  
    namespaces 174–175  
    tenant 109  
Allow lists  
    about 182  
    adding IP addresses 182  
    CIFS protocol handling of 184  
    deleting IP addresses 182  
    HS3 API handling of 183  
    HTTP protocol handling of 183  
    NFS protocol handling of 184  
    SMTP protocol handling of 184  
    valid entries 182–183  
    WebDAV protocol handling of 183  
allow namespace management property  
    about 62  
    assigning to group accounts 85  
    assigning to user accounts 79  
    changing for user and group accounts 86  
allowing  
    See also [enabling](#)  
    namespace access by IP addresses 182–184  
    ownership and permission changes for  
        objects under retention 161–163  
annotations  
    See also [custom metadata](#)  
    about 2

annotations, excluding from indexing

- excluding from indexing 237
- with XPath expressions 214–215
- appendable objects
  - about 3, 24
  - enabling/disabling 166–167
- associating
  - content classes with namespaces 236, 238–239
  - namespaces with content classes 232–233
  - service plans with namespaces 148, 169–170
  - tags with namespaces 147, 154–155
- atime synchronization
  - about 24
  - enabling/disabling 166–167
- authentication
  - See [user authentication](#)
- automatic deletion
  - See [disposition](#)

## B

- basic authentication, WebDAV 190
- Boolean data type 215
- browse permission
  - data access permissions 69
  - minimum data access permissions 29

## C

- case forcing, CIFS protocol 193, 194
- case sensitivity, CIFS protocol 192–193, 194
- change owner permission 69
- Change Password page 55–56
- changing
  - See also [configuring](#); [modifying](#); [setting](#)
  - allow namespace management property for user and group accounts 86
  - appendable objects setting 166–167
  - atime synchronization setting 166–167
  - CIFS case sensitivity 192–193, 194
  - collision handling option 168–169
  - compatibility properties 166–167
  - custom metadata operations allowed for objects under retention 161–163
  - default index setting 158–159
  - default POSIX GID 196
  - default POSIX UID 195
  - default retention setting 156–157
  - default settings for namespace creation 171–173
  - default shred setting 157–158

- enforce ACLs setting 161
- hard quota for namespaces 152–153
- limit on namespace ownership 173–174
- login settings 92–93
- minimum data access permissions 159–160
- namespace descriptions 152
- namespace names 150–151
- namespace owners 153–154
- namespace permission masks 151–152
- ownership and permission changes for objects under retention, setting for 161–163
- passwords 55–56
- retention class values 245
- retention mode 170–171
- retention-related properties 161–163
- service plans for namespaces 169–170
- soft quota for namespaces 152–153
- tags associated with namespaces 154–155
- tenant contact information 102–103
- tenant description 104
- tenant permission mask 103–104
- Chargeback page 129
- chargeback reports
  - about 127–128
  - content 130–132
  - deleted namespaces 177
  - generating 129
  - HCP management API 129
  - sample 132–133
  - statistics collection 129
  - status of statistics 132
  - types 128–129
- CIFS panel 191–192, 194
- CIFS protocol
  - about 5–6
  - Allow/Deny list handling 184
  - Allow/Deny lists 182
  - authentication 192
  - case forcing 193, 194
  - case sensitivity 192–193, 194
  - configuring 191–192, 194–195
  - object representation 11
  - user authentication 184–185
  - with Windows workgroups 192
- collision handling
  - See [replication collisions](#)
- Compatibility panel 166–167
- compatibility properties
  - about 24–25
  - changing 166–167

- compliance activities, performing 60
- Compliance Events panel
  - namespaces 175
  - tenant 110
- compliance mode 17
  - See also* [retention mode](#)
- compliance role 65
- configuration collisions 42–44
- configuring
  - See also* [changing](#); [modifying](#); [setting](#)
  - CIFS protocol 191–192
  - email notification 114–121
  - Firefox for single sign-on 271
  - HS3 API 185–191
  - HTTP protocol 185–191
  - Internet Explorer for single sign-on 270–271
  - Microsoft Exchange 2003 for SMTP 199–200
  - Microsoft Exchange 2007 for SMTP 201–202
  - Microsoft Exchange 2010 for SMTP 202
  - namespace access protocols 180
  - namespaces 149–150
  - NFS protocol 195–196
  - SMTP protocol 196–198
  - tenant 101
  - WebDAV protocol 185–191
- Console pages
  - See also* [Tenant Management Console](#)
  - Change Password 55–56
  - Chargeback 129
  - Console Security 90–91, 105–106
  - Email 115–121
  - Groups 81–90
  - Idle Timeout 49, 92
  - login 52–53
  - Management API 106–107
  - Miscellaneous 174
  - Namespace Defaults 171–173
  - Namespaces 136–138
  - Overview, tenant 96–101
  - refreshing 54
  - Replication 121–127
  - Search Security 107
  - SNMP 114
  - Syslog 113
  - Tenant Events 109–110
  - Users 74–81, 86–90
- Console Security page
  - changing user account and login
    - settings 90–91
  - controlling access to Tenant Management
    - Console 105–106
- contact information
  - changing 102–103
  - viewing 100
- Contact Information window 102–103
- content classes
  - about 206
  - alerts 257
  - associating/dissociating with
    - namespaces 232–233, 236, 238–239
  - creating 228
  - deleting 235–236
  - list 226–227
  - managing content properties 228–231
  - names 208, 228
  - reindexing namespaces associated with 232, 233–235
  - renaming 235
  - workflow 208–209
- content properties
  - about 206
  - adding 228–229
  - adding individually 229
  - data types 215–216
  - definitions 209–210
  - definitions in content property files 223–225
  - deleting 228–229
  - exporting 231
  - expressions 212–215
  - extracted from XML 221–223
  - extracting from XML 230
  - importing 230
  - indexing 207
  - list 227
  - modifying 228–229
  - multivalued 221
  - names 210–212
  - testing 231
  - workflow 208–209
- content property files
  - about 223–225
  - exporting content properties to 231
- controlling
  - access to Search Console 107
  - access to Tenant Management
    - Console 105–106
  - HCP management API access 106–107
  - namespace access through CIFS 194
  - namespace access through HS3 191
  - namespace access through HTTP 191
  - namespace access through NFS 196
  - namespace access through SMTP 197
  - namespace access through WebDAV 191
- Create Group Accounts panel 84–85
- Create Namespace panel 145–149
- Create Retention Class panel 244

Create User Account panel 77–79

creating

*See also* [adding](#)

content classes 228

group accounts 83–85

namespaces 58, 144–149

namespaces, default settings for 171–173

retention classes 244

user accounts 77–79

cryptographic hash algorithms

about 16

changing default for namespace creation 171

setting 146

viewing 143

cryptographic hash values 16

current tenant 53

custom metadata

*See also* [annotations](#)

about 2

collisions 39–41

enabling/disabling full indexing 237,  
238–239

enabling/disabling indexing 236–237,  
238–239

indexing by metadata query engine 207

indexing, about 204–205

operations allowed for objects under  
retention, about 22–23

operations allowed for objects under  
retention, changing 161–163

sample 210

XML checking, about 23

XML checking, enabling/disabling 163

## D

daily chargeback reports 128

data access permission masks 26–28

*See also* [namespace permission masks](#);  
[tenant permission mask](#)

data access permissions

*See also* [permissions](#)

about 69–70

changing 86–90

minimum 28–30, 159–160

namespace owners 18

removing all for individual namespaces 90

data directory 11

Data Migrator

*See* [HCP Data Migrator](#)

data protection level

*See* [DPL](#)

data transmission rate, replication 124–125

data types for content properties

about 215–216

formats 216–221

datetime data type

about 216

formats 219–221

default email message template 118–119

default index setting

about 20–21

changing 158–159

default POSIX GID

about 21–22

changing 196

default POSIX permissions 21

default POSIX UID

about 21–22

changing 195

default retention setting

about 19

changing 156–157

valid values 155–156

default settings for namespace creation 171–173

default shred setting

about 20

changing 157–158

delete permission

ACLs 31

data access permission masks 26

data access permissions 69

minimum data access permissions 30

deleting

*See also* [removing](#)

content classes 235–236

content properties 228–229

email recipients 120–121

group accounts 85–86

IP addresses from Allow/Deny lists 182

irreparable objects 176

namespaces 177–178

objects under retention 248–250

retention classes 245–246

user accounts 80–81

Deletion Allowed 19, 155, 242

Deletion Prohibited 156, 242

Deny lists

about 182

adding IP addresses 182

CIFS protocol handling of 184

deleting IP addresses 182

HS3 protocol handling of 183

HTTP protocol handling of 183

SMTP protocol handling of 184

valid entries 182–183

WebDAV protocol handling of 183

- denying
    - See also* [disabling](#)
    - namespace access by IP addresses 182–184
    - ownership and permission changes for
      - objects under retention 161–163
  - descriptions
    - namespaces, changing 152
    - namespaces, changing default for
      - namespace creation 171
    - namespaces, specifying initially 146
    - namespaces, viewing 144
    - retention classes 244
    - tenant, changing 104
    - user accounts 78
  - deselecting namespaces for replication 125–127, 168
  - directories
    - data 11
    - metadata 11
    - rest 9
  - disabled user accounts 77
  - disabling
    - See also* [denying](#)
    - appendable objects 166–167
    - atime synchronization 166–167
    - custom metadata indexing 236–237, 238–239
    - custom metadata XML checking 163
    - disposition 167
    - full custom metadata indexing 237, 238–239
    - indexing 236, 238–239
    - read from remote system 168–169
    - replication for namespaces 148
    - search 148, 205–206, 236, 238–239
    - service by remote systems 168–169
    - system-level administrative access to
      - tenants 104–105
    - user accounts 63, 79
    - user accounts automatically 91
    - versioning 148–149, 165
  - disposition
    - about 25
    - automatic deletion of objects in retention
      - classes 242
    - enabling/disabling 167
  - Disposition panel 167
  - dissociating
    - content classes from namespaces 236, 238–239
    - namespaces from content classes 232–233
    - namespaces from user/group accounts 90
  - documentation, viewing 55
  - downloading
    - HCP Data Migrator 252
    - HCP documentation 55
  - DPL
    - about 15–??
    - changing default for namespace creation 171
    - dynamic 16
    - and replication 146
    - setting 146
    - viewing 144
  - dynamic
    - DPL 16
    - statistics 129
- ## E
- Edit Retention Class window 245
  - effective permission mask
    - namespaces 144
    - tenant 100
  - email
    - See also* [email notification](#)
    - archiving 196
    - storing attachments 196–197
  - email message template
    - See also* [email notification](#)
    - about 116–117
    - default 118–119
    - modifying 117
    - variables 117–118
  - email notification
    - about 114–115
    - enabling 115
    - message template 116–119
    - recipients 119–121
    - testing 115–116
  - Email page 115–121
  - email recipients 119–121
    - See also* [email notification](#)
  - enabling
    - See also* [allowing](#)
    - ACLs 160–161
    - appendable objects 166–167
    - atime synchronization 166–167
    - CIFS protocol 194–195
    - custom metadata indexing 236–237, 238–239
    - custom metadata XML checking 163
    - disposition 167
    - email notification 115
    - full custom metadata indexing 237, 238–239
    - HS3 API 189
    - HS3 use for namespace management 106
    - HTTP protocol 188–190
    - indexing 236, 238–239

enabling, NFS protocol

- NFS protocol 195–196
- read from remote system 168–169
- replication for namespaces 148
- search 148, 205–206, 236, 238–239
- service by remote systems 168–169
- SMTP protocol 197–198
- system-level administrative access to
  - tenant 104–105
- user accounts 63, 79
- versioning 148–149, 165
- WebDAV protocol 189–190
- enforcing ACLs
  - about 31
  - changing setting for 161
- enterprise mode 17
  - See also* [retention mode](#)
- Error (event severity) 112
- ETags 187
- events
  - See also* [log messages](#)
  - initiator 111, 112
  - severity 111–112
- excluding annotations from indexing 237
- expired objects, automatic deletion 25
- expired passwords 91
- exported content properties 223–225
- exporting content properties 231
- expressions for content properties 212–215
- extracted content properties 221–223
- extracting content properties from XML 230

## F

- failed logins to namespaces 63
- features
  - namespaces 143
  - tenant 98–99
- files
  - hosts 50–51
  - objects stored for 2–3
- filtering
  - content class list 227
  - group account list 83
  - namespace list 137–138
  - namespace list on Replication page 123
  - user account list 76
- Firefox, configuring for single sign-on 271
- fixed content 2
- fixed date as default retention setting 156
- float data type
  - about 216
  - formats 217–218
- forcing password changes 78, 91
- formats for content properties

- datetime data type 219–221
- float data type 217–218
- integer data type 216–217
- full custom metadata indexing
  - about 207
  - enabling/disabling 237, 238–239

## G

- generating chargeback reports 129
- GID
  - See* [POSIX GID](#)
- group accounts
  - about 62, 63
  - allow namespace management property,
    - about 62
  - allow namespace management property,
    - assigning 85
  - allow namespace management property,
    - changing 86
  - changing data access permissions 86–90
  - creating 83–85
  - deleting 85–86
  - list 82–83
  - managing 57
  - maximum number 63
  - modifying 85
  - names 83
  - names with deleted Active Directory
    - groups 86
  - number of 97
- Groups page
  - about 81–83
  - changing allow namespace management
    - property 86
  - changing data access permissions 86–90
  - creating group accounts 84–85
  - deleting group accounts 86
  - modifying group accounts 85
- groups, Active Directory, creating HCP group
  - accounts from 83–85

## H

- hard quota
  - about 14–15
  - changing default for namespace creation 172
  - namespaces, changing 152–153
  - namespaces, setting initially 147
  - namespaces, viewing 136, 141
  - tenant, viewing 96, 136
- hash algorithms
  - See* [cryptographic hash algorithms](#)
- hash values 16



- HCP
    - about 1–2
    - documentation 55
    - email archiving 196
    - file system 11
    - service by remote systems 33, 168–169
    - version 52
  - HCP Data Migrator
    - about 8–9
    - downloading 252
    - system requirements 252
  - HCP group accounts
    - See [group accounts](#)
  - HCP management API
    - about 49–50
    - chargeback reports 129
    - controlling access to 106–107
  - HCP search facility
    - indexing 204–205
  - HCP user accounts
    - See [user accounts](#), [HCP](#)
  - HCP-DM
    - See [HCP Data Migrator](#)
  - HCP-FS 11
  - HDDS search facility
    - about 8
    - indexing 205
  - Hitachi Content Platform
    - See [HCP](#)
  - Hitachi Data Discovery Suite
    - See [HDDS search facility](#)
  - hostname mappings 51
  - hosts file 50–51
  - hourly chargeback reports 128
  - HS3 API
    - about 5–6
    - Allow/Deny list handling 183
    - Allow/Deny lists 182
    - configuring 185–191
    - considerations 187
    - enabling use of for namespace management 106
    - object representation 10, 10
    - SSL security 188
    - user authentication 184–185
  - HTTP protocol
    - about 5–6
    - Allow/Deny list handling 183
    - Allow/Deny lists 182
    - configuring 185–191
    - object representation 9
    - SSL security 188
    - user authentication 184–185
  - HTTP(S) panel 185–191
  - HTTPS protocol
    - See [HTTP protocol](#)
- ## I
- Idle Timeout page 49, 92
  - importing content properties 230
  - inactive user accounts 92
  - index settings
    - about 20
    - default 20–21
  - indexes
    - See also [indexing](#); [search](#)
    - about 204–206
    - objects included in 20–21
  - indexing
    - See also [indexes](#); [search](#)
    - about 8, 204–206
    - custom metadata by metadata query engine 207
    - custom metadata, about 204–205
    - enabling/disabling 236, 238–239
    - excluding annotations 237
  - Indexing panel 159
  - ingested volume 141
  - Initial Unspecified 156, 242
  - integer data type
    - about 215–216
    - formats 216–217
  - Internet Explorer, configuring for single sign-on 270–271
  - IP addresses
    - in Allow/Deny lists 182–183
    - for HCP system 51
  - irreparable objects
    - acknowledging 176–177
    - deleting 176
    - viewing 175–176
  - Irreparable Objects panel 175–177
- ## K
- keeping deletion records 164
- ## L
- limit on namespace ownership
    - about 18
    - changing 173–174
  - local authentication 71
  - log messages
    - about 111–112
    - descriptions 259–268
    - details 112

log messages, event severity

- event severity 111–112
- importance 114
- managing list of 112–113
- sending through email 114–115
- sending to SNMP managers 113–114
- sending to syslog servers 113
- types 114
- viewing 108–109

logging into Tenant Management Console 51–52

logging out of Tenant Management Console 56

login settings

- about 91–92

- changing 92–93

## M

Mac OS X hosts file 50

maintaining

- namespaces 58

- tenant 57

major events

- See also* [log messages](#)

- namespaces 142

- tenant 97–98

Management API page 106–107

managing

- content class list 226–227

- content properties 228–231

- group account list 82–83

- group accounts 57

- namespace access 60

- namespace list 137–138

- tenant log message list 112–113

- user account list 76

- user accounts 57

mappings, hostname 51

maximum

- content classes per tenant 208

- group accounts per tenant 63

- namespaces per tenant 4

- namespaces per user 173–174

- tenants per HCP system 4

- user accounts per tenant 63

message text for Console login pages 92

metadata

- See also* [ACLs](#); [custom metadata](#)

- about 2–3

- ACLs 2–3

- custom 2

- system 2

metadata directory 11

Metadata panel 163

metadata query API 6–7

metadata query engine

- about 8

- custom metadata indexing 207

- indexing 204–205

Metadata Query Engine Console 8

metafiles 11

Microsoft Exchange, configuring for SMTP

- considerations for mixed Exchange 2003 and 2010 environments 199

- Exchange 2003 199–200

- Exchange 2007 201–202

- Exchange 2010 202

minimum data access permissions

- about 28–30

- changing 159–160

minimum length for passwords 91

Miscellaneous page 174

Modify Namespace Quota window 153

modifying

- See also* [changing](#); [configuring](#); [setting](#)

- content properties 228–229

- email recipients 120–121

- group accounts 85

- retention classes 245

- user accounts 79–80

monitor role 64

monitoring

- namespaces 58–60, 174

- replication 121–125

- tenant 58–60, 108–109

monthly chargeback reports 128

Mozilla Firefox, configuring for single sign-on 271

multivalued content properties 221

## N

Name panel 151

names

- content classes 208, 228

- content properties 210–212

- group accounts 83

- group accounts with deleted Active Directory groups 86

- namespaces, about 145–146

- namespaces, changing 150–151

- retention classes 244

- usernames 77

namespace access protocols

- See also* [CIFS protocol](#); [HS3 API](#); [HTTP protocol](#); [NFS protocol](#); [SMTP protocol](#); [WebDAV protocol](#)

- about 5–6

- Allow/Deny lists 182

- authentication required 5

- configuring 180

- Namespace Browser 6
- Namespace Defaults page 171–173
- namespace permission masks
  - See also* [data access permission masks](#)
  - about 27
  - changing 151–152
  - viewing 144
- namespace quota 96
- namespace-level view of replication 123–125
- namespaces
  - about 3
  - access to 4
  - alerts 136, 142, 255–257
  - all events 174–175
  - allowing/denying access by IP
    - addresses 182–184
  - allowing/denying ownership and permission
    - changes for objects under retention, about 22
  - allowing/denying ownership and permission
    - changes for objects under retention, changing setting for 161–163
  - associating/dissociating content classes
    - with 236, 238–239
  - associating/dissociating with content
    - classes 232–233
  - changing data access permissions for
    - individual 89–90
  - changing data access permissions for
    - multiple 87–88
  - changing ownership limit 173–174
  - chargeback reports 127
  - CIFS access, enabling/disabling 194–195
  - collision handling option, changing 168–169
  - compatibility properties, about 24–25
  - compatibility properties, changing 166–167
  - compliance events 175
  - configuring 149–150
  - creating 58, 144–149
  - cryptographic hash algorithm, about 16
  - cryptographic hash algorithm, changing
    - default for namespace creation 171
  - cryptographic hash algorithm, setting 146
  - cryptographic hash algorithm, viewing 143
  - custom metadata operations allowed for
    - objects under retention, about 22–23
  - custom metadata operations allowed for
    - objects under retention, changing 161–163
  - custom metadata XML checking, about 23
  - custom metadata XML checking,
    - enabling/disabling 163
  - default index setting, about 20–21
  - default index setting, changing 158–159
  - default retention setting, about 19
  - default retention setting, changing 156–157
  - default settings for creation 171–173
  - default shred setting, about 20
  - default shred setting, changing 157–158
  - deleting 177–178
  - description, changing 152
  - description, changing default for namespace
    - creation 171
  - description, specifying initially 146
  - description, viewing 144
  - disposition, about 25
  - disposition, enabling/disabling 167
  - dissociating from user/group accounts 90
  - DPL, about 15–??
  - DPL, changing default for namespace
    - creation 171
  - DPL, setting initially 146
  - DPL, viewing 144
  - effective permissions 27
  - enabling/disabling search 236, 238–239
  - failed logins 63
  - features 143
  - filtering list of 137–138
  - hard quota, about 136
  - hard quota, changing 152–153
  - hard quota, changing default for namespace
    - creation 172
  - hard quota, setting initially 147
  - hard quota, viewing 141
  - HS3 access, enabling/disabling 189
  - HTTP access, enabling/disabling 188–190
  - indexed object count 140–141
  - indexing 204–206
  - list 136–138
  - list on Replication page 122–123
  - log messages 174–175
  - maintaining 58
  - major events 142
  - managing access to 60
  - maximum number 4
  - minimum data access permissions,
    - about 28–30
  - minimum data access permissions,
    - changing 159–160
  - monitoring 58–60, 174
  - names, about 145–146
  - names, changing 150–151
  - NFS access, enabling/disabling 195–196
  - number of 96
  - object count 136, 140–141
  - owners, about 3, 18–19

- owners, changing 153–154
- owners, setting initially 146
- owners, viewing 139–140
- paging through list of 137
- permission mask, changing 151–152
- permission mask, viewing 144
- pruning, changing defaults for namespace creation 172–173
- quota 14
- read from remote system, about 33
- read-only 28
- reindexing individual 237, 239–240
- reindexing multiple 232, 233–235
- reindexing, about 208–209
- renaming 150–151
- replication, about 34
- replication, changing default for namespace creation 172
- replication, enabling/disabling 148
- replication, viewing 143
- retention mode, about 17
- retention mode, changing 170–171
- retention mode, changing default for namespace creation 172
- retention mode, setting initially 148
- retention mode, viewing 143
- search and indexing options 236–237
- search enabled 204
- search feature, changing default for namespace creation 172
- search feature, setting initially 148
- search feature, viewing 143
- secure 5
- selecting/deselecting for
  - replication 125–127, 168
- service by remote systems, about 33
- service by remote systems,
  - enabling/disabling 168–169
- service plan, changing 169–170
- service plan, setting initially 148
- service plan, viewing 143
- service plans, changing default for namespace creation 172
- SMTP access, enabling/disabling 197–198
- soft quota, changing 152–153
- soft quota, changing default for namespace creation 172
- soft quota, setting initially 147
- sorting list of 137
- statistics in chargeback reports 130–132
- storage quotas 14–15
- storage usage 136, 141
- tags, about 19

- tags, changing 154–155
- tags, setting initially 147
- URLs 138–139
- versioning, about 23–24
- versioning, changing default for namespace creation 172
- versioning, enabling/disabling 165
- versioning, enabling/disabling initially 148–149
- versioning, viewing 143
- WebDAV access, enabling/disabling 189–190

Namespaces page

- about 136–138
- ACLs panel 161
- alerts 255–256
- All Events panel 174–175
- changing namespace quotas 153
- CIFS panel 191–192, 194
- Compatibility panel 166–167
- Compliance Events panel 175
- Create Namespace panel 145–149
- Create Retention Class panel 244
- deleting namespaces 178
- Disposition panel 167
- HTTP(S) panel 185–191
- Indexing panel 159
- Irreparable Objects panel 175–177
- Metadata panel 163
- namespace list 136–138
- NFS panel 195–196
- Overview panel 138–144, 152
- Permissions panel 159–160
- Privileged Delete panel 249–250
- Replication panel 168–169
- Retention Classes panel 243
- Retention Mode panel 171
- Retention panel 156–157, 162
- Search panel 237–240
- Service Plan panel 169–170
- Shredding panel 158
- SMTP panel 196–198
- Versioning panel 165

Namespaces panel (Search page) 232–233

NFS panel 195–196

NFS protocol

- about 5–6
- Allow list handling 184
- Allow lists 182
- configuring 195–196
- object representation 11

Notice (event severity) 111

**O**

object versioning

See [versioning](#)

objects

- about 2–3
- allowing/denying ownership and permission changes under retention 22
- appendable 3
- automatic deletion 25, 167
- content collisions, about 34–35
- content collisions, handling 168–169
- hash value 16
- index setting 20–21
- indexed per tenant 97
- list of irreparable 175–176
- number of indexed over time 140–141
- number of over time 140–141
- number of per namespace 136
- number of per tenant 97
- ownership 21, 22
- POSIX UID, GID, and permissions 21–22
- representation with HS3 API 10, 10
- representation with HTTP protocol 9
- representation with WebDAV, CIFS, and NFS protocols 11
- retention setting 16, 19
- shred setting 20
- specifying for privileged delete 248–249
- versions 3

operation rate, replication 125

Overview page, tenant

- alerts 254
- changing tenant contact information 102–103
- changing tenant descriptions 104
- changing tenant permission masks 103–104
- enabling/disabling system-level administrative access 105
- understanding 96–101

Overview panel, namespace

- about 138–144
- alerts 256–257
- changing namespace descriptions 152
- changing namespace owners 153–154
- changing namespace permission masks 151–152

owners, namespace

- about 18–19
- changing 153–154
- data access permissions 18
- setting initially 146
- viewing 139–140

ownership and permission changes for objects under retention

- about 22
- allowing/denying 161–163

**P**

paging

- content class list 226
- group account list 82–83
- namespace list 137
- namespace list on Replication page 122–123
- user account list 76

passwords

- Active Directory authenticated users 72–73
- changing your own 52, 55–56
- expiration 91
- forcing changes 78, 91
- HCP user accounts, about 55–56, 78
- locally authenticated users 71
- minimum length 91
- RADIUS-authenticated users 72

percent encoding for privileged delete 249

performing

- compliance activities 60
- privileged delete operations 249–250

permissions

See also [data access permissions](#); [POSIX permissions](#)

- Active Directory users 48
- granted by roles 65–68

Permissions panel 159–160

point-in-time statistics 129

ports, HTTP and HTTPS 188

POSIX GID

- about 21
- allowing/denying changes for objects under retention 161–163
- changing default 196

POSIX permissions

- about 21
- allowing/denying changes for objects under retention 161–163

POSIX UID

- about 21
- allowing/denying changes for objects under retention 161–163
- changing default 195

privileged delete

- about 247–248
- object specification 248–249
- performing 249–250

Privileged Delete panel 249–250

privileged permission

privileged permission

- data access permission masks 26

- data access permissions 70

privileged purge 248

- See also* [privileged delete](#)

Protocols panel 180

pruning

- about 24, 164

- changing defaults for namespace

  - creation 172–173

- configuring 165

purge permission

- data access permission masks 26

- data access permissions 69

- minimum data access permissions 30

## Q

quotas

- See* [hard quota](#); [namespace quota](#); [soft quota](#)

## R

RADIUS authentication 72

read ACL permission

- ACLs 31

- data access permissions 69

- minimum data access permissions 29

read from remote system

- about 33

- enabling/disabling 168–169

read permission

- ACLs 30

- data access permission masks 26

- data access permissions 69

- minimum data access permissions 29

read-only tenants 98

recipients, email 119–121

recognized Active Directory user accounts 48

refreshing Console pages 54

Reindex panel (Search page) 233–235

reindexing

- about 208–209

- namespaces associated with content

  - classes 232, 233–235

- namespaces individually 237, 239–240

remote authentication 71

removing

- See also* [deleting](#)

- namespace owners 153–154

- tags from namespaces 154–155

renaming

- content classes 235

- namespaces 150–151

replication

- about 32, ??–34

- benefits 32–33

- changing default for namespace creation 172

- collision handling 34–45, 168–169

- data transmission rate 124–125

- deleting replicated namespaces 177

- and DPL 146

- implementation 33–34

- monitoring 121–125

- namespace-level view 123–125

- namespaces, enabling/disabling initially 148

- namespaces, viewing 143

- operation rate 125

- selecting/deselecting namespaces

  - for 125–127, 168

- service by remote systems 33, 168–169

- tenant eligibility 98

- tenant-level view 121–122

- topologies 32

- up-to-date-as-of time 122, 124

replication collisions

- about 34

- ACLs 41–42

- automatic deletion 25

- configuration 42–44

- custom metadata 39–41

- object content, about 34–35

- object content, handling 168–169

- retention classes 44–45

- system metadata 36–38

Replication page, tenant 121–127

Replication panel, namespace 168–169

reports, chargeback 127–133

reserved words, content property names 212

responsibilities, tenant administrator 56–60

REST API

- See* [HTTP protocol](#)

rest directory 9

restoring default email message

- template 118–119

retention classes

- about 241–242

- automatically deleting expired objects in 242

- collisions 44–45

- creating 244

- deleting 245–246

- description 244

- list 243

- modifying 245

- names 244

Retention Classes panel 243

- retention mode
  - about 17
  - changing 170–171
  - changing default for namespace creation 172
  - selection 99
  - setting initially 148
  - viewing 143
- Retention Mode panel 171
- Retention panel
  - default retention setting 156–157
  - retention-related settings 162
- retention periods 16
- retention settings
  - about 16
  - default 19
- retention-related properties
  - about 22
  - changing 161–163
- roles
  - about 64–65
  - Active Directory users 64, 70
  - administrator 64
  - changing for group accounts 85
  - changing for user accounts 79–80
  - compliance 65
  - monitor 64
  - permissions granted by 65–68
  - security 64–65

## S

- sample custom metadata
  - about 210
  - content properties extracted from 222–223
  - exported content property definitions 224–225
- search
  - See also* [indexes](#); [indexing](#)
  - about 204–206
  - changing default for namespace creation 172
  - enabling/disabling 236, 238–239
  - namespace feature 143
  - tenant feature 99
  - viewing for namespaces 148
- Search Console
  - about 7–8
  - controlling access to 107
  - login page message text 92
- search facilities
  - See also* [HCP search facility](#); [HDDS search facility](#); [metadata query engine](#)
  - about 8
  - indexes 8
- search indexes
  - See* [indexes](#)
- Search page
  - about 226–227
  - adding content properties 229
  - adding content properties individually 229
  - alerts 257
  - associating/dissociating namespaces with content classes 232–233
  - creating content classes 228
  - deleting content classes 235–236
  - deleting content properties 229
  - exporting content properties 231
  - extracting content properties from XML 230
  - importing content properties 230
  - modifying content properties 229
  - reindexing namespaces 233–235
  - renaming content classes 235
  - testing content properties 231
- Search panel (namespaces)
  - displaying 237–238
  - reindexing namespaces 239–240
  - setting search and indexing options 238–239
- search permission
  - data access permission masks 27
  - data access permissions 70
- Search Security page 107
- search-enabled namespaces 204
- secure deletion 20
- secure namespaces 5
- Security Events panel 110
- security role 64–65
- selecting namespaces for replication 125–127, 168
- service by remote systems
  - about 33
  - enabling/disabling 168–169
- Service Plan panel 169–170
- service plans
  - about 45–46
  - associating with namespaces 148, 169–170
  - changing default for namespace creation 172
  - viewing 143
- session timeout 92
- setting
  - See also* [changing](#); [configuring](#); [modifying](#)
  - cryptographic hash algorithm 146
  - DPL 146
  - hard quota for namespaces 147
  - retention mode 148
  - soft quota for namespaces 147
- Settings panel (Search page)
  - about 227
  - adding content properties 228–229



- adding content properties individually 229
  - deleting content properties 228–229
  - exporting content properties 231
  - extracting content properties from XML 230
  - importing content properties 230
  - modifying content properties 228–229
  - renaming content classes 235
  - testing content properties 231
  - severity, events 111–112
  - shortcut keys 53
  - shred setting, default 20
  - shredding 20
    - See also* [default shred setting](#)
  - Shredding panel 158
  - single sign-on
    - about 48, 72
    - configuring Firefox for 271
    - configuring Internet Explorer for 270–271
  - SMTP panel 196–198
  - SMTP protocol
    - about 5
    - Allow/Deny list handling 184
    - Allow/Deny lists 182
    - configuring 196–198
    - with Microsoft Exchange 198–202
  - SNMP logging 113–114
  - SNMP page 114
  - soft quota
    - about 14–15
    - changing default for namespace creation 172
    - namespaces, changing 152–153
    - namespaces, setting initially 147
  - sorting
    - content class list 227
    - group account list 83
    - namespace list 137
    - namespace list on Replication page 123
    - user account list 76
  - specifying
    - days for version pruning 149, 165
    - namespace descriptions 146
    - objects for privileged delete 248–249
  - SPNEGO 73
  - SSL security with HTTP, HS3, and WebDAV
    - protocols 188
  - starter account 73–74
  - statistics
    - in chargeback reports 130–132
    - collection for chargeback reports 129
    - dynamic 129
    - point in time 129
    - status in chargeback reports 132
  - tenant 96–97
  - storage
    - amount used per object 16
    - namespace usage 136, 141
    - object based 2–3
    - tenant usage 96
  - string data type 215
  - submitting changes in Tenant Management Console 54
  - syslog logging 113
  - Syslog page 113
  - system metadata 2
  - system metadata collisions 36–38
  - system-level administrative access to tenant
    - about 46
    - enabling/disabling 104–105
  - systemwide permission mask 27
- ## T
- tags
    - about 19
    - associating with namespaces 147
    - changing for namespaces 154–155
    - removing from namespaces 154–155
  - template, email message 116–119
  - tenant administrators
    - responsibilities 56–60
    - roles 64–65
  - Tenant Events page
    - All Events panel 109
    - Compliance Events panel 110
    - Security Events panel 110
  - tenant log
    - See also* [log messages](#); [Tenant Events page](#)
    - about 108–109
    - namespace view of 174–175
  - Tenant Management Console
    - See also* [Console pages](#)
    - about 48
    - access 48
    - controlling access to 105–106
    - logging in 51–52
    - logging out 56
    - login page message text 92
    - session timeout 92
    - sessions 48–49
    - starter account 73–74
    - submitting changes 54
    - system-level administrative access to 49
    - tenant description on login page 100–101
    - URL 50
    - using 53–54



## tenant permission mask

See also [data access permission masks](#)

about 27

changing 103–104

viewing 100

## tenant-level view of replication 121–122

## tenants

about 3–4

administrator responsibilities 56–60

alerts 98, 254

all events 109

compliance events 110–111

configuring 101

contact information, changing 102–103

contact information, viewing 100

current 53

description, changing 104

description, viewing 100–101

effective permissions 27

features 98–99

hard quota 96, 136

maintaining 57

major events 97–98

maximum number 4

monitoring 58–60, 108–109

namespace quota 14, 96

permission mask, about 100

permission mask, changing 103–104

read-only 98

replication 33–34, 98

search support 99

security events 110

service plan selection 99

statistics 96–97

statistics in chargeback reports 130–132

storage quotas 14–15

system-level administrative access to,  
about 46

system-level administrative access to,  
enabling/disabling 104–105

versioning 99

testing content properties 231

testing email notification 115–116

text for Console login pages 92

tokenized data type 215

transaction log 164

transfer rate, replication 124–125

**U**

## UID

See [POSIX UID](#)

Unix hosts file 50

up-to-date-as-of time, replication 122, 124

## URLs

namespaces 138–139

Tenant Management Console 50

## user accounts, Active Directory

logging in 51–52

recognized 48

username change 54

## user accounts, HCP

about 62–63

alerts 258

allow namespace management property,  
about 62

allow namespace management property,  
assigning 79

allow namespace management property,  
changing 86

changing data access permissions 86–90

creating 77–79

deleting 80–81

disabled 77

disabling automatically 91

enabling/disabling 63, 79

inactive 92

list 75–76

managing 57

maximum number 63

modifying 79–80

number of locally authenticated 97

number of RADIUS-authenticated 97

starter 73–74

user ID 79

## user authentication

about 70–71

Active Directory 72–73

CIFS protocol 184–185

HS3 API 184–185

HTTP protocol 184–185

local 71

RADIUS 72

## usernames 77

## Users page

about 74–76

alerts 258

changing allow namespace management  
property 86

changing data access permissions 86–90

creating user accounts 77–79

deleting user accounts 81

modifying user accounts 80

using Tenant Management Console 53–54

**V**

variables, email message template 117–118

version pruning

version pruning

See [pruning](#)

version, HCP 52

versioning

about 3, 23–24, 164

changing default for namespace creation 172

enabling/disabling 148–149, 165

namespace feature 143

privileged purge 248

pruning 24, 149

specifying days for pruning 165

tenant feature 99

Versioning panel 165

viewing

all namespace events 174–175

all tenant events 109

HCP documentation 55

irreparable objects 175–176

namespace compliance events 175

namespace descriptions 144

namespace permission masks 144

namespace retention modes 143

namespace service plans 143

tenant compliance events 110–111

tenant contact information 100

tenant description 100–101

tenant permission mask 100

tenant security events 110

volume, ingested 141

data access permission masks 26

data access permissions 69

minimum data access permissions 29

## X

XML checking for custom metadata

about 23

enabling/disabling 163

XML, extracting content properties from 230

XPath expressions

about 212–215

annotation specific 214–215

## W

Warning (event severity) 112

WebDAV protocol

about 5–6

Allow/Deny list handling 183

Allow/Deny lists 182

basic authentication 190

configuring 185–191

object representation 11

SSL security 188

Windows

case sensitivity 192–193

hosts file 50

workgroups 192

Windows Internet Explorer, configuring for single

sign-on 270–271

WORM 2

write ACL permission

ACLs 31

data access permissions 69

minimum data access permissions 29

write permission

ACLs 31



## **Hitachi Data Systems**

### **Corporate Headquarters**

2845 Lafayette Street  
Santa Clara, California 95050-2627  
U.S.A.  
[www.hds.com](http://www.hds.com)

### **Regional Contact Information**

#### **Americas**

+1 408 970 1000  
[info@hds.com](mailto:info@hds.com)

#### **Europe, Middle East, and Africa**

+44 (0) 1753 618000  
[info.emea@hds.com](mailto:info.emea@hds.com)

#### **Asia Pacific**

+852 3189 7900  
[hds.marketing.apac@hds.com](mailto:hds.marketing.apac@hds.com)



MK-99ARC025-13