

Workshare Hybrid Storage

INSTALLATION GUIDE

Table of Contents

Introduction.....	4
Secure Workshare cloud deployment.....	4
Hybrid cloud deployment.....	5
Environment Requirements	5
Application Server	6
File Content Storage	6
Databases.....	7
Network Environment.....	7
Considerations for Production/Testing Environments	8
Setup Overview	9
Evaluation Mode and Production Mode	9
Deploying Workshare Hybrid Storage.....	10
Prerequisites	10
Installation Process	10
Step 1: Obtain and unpack the Workshare.HybridStorage-<VersionNumber>.zip file	10
Step 2: Edit the 'Configuration.ps1' file.....	11
Step 3: Run the 'SetupServer.ps1' file.....	11
Script Configuration Options.....	11
Deploying an Evaluation/Testing Environment	13
Deploying a Production Environment.....	14
Upgrading Workshare Hybrid Storage	14
Upgrading Existing Server	14
Step 1: Back up install folder	15
Step 2: Confirm configuration settings.....	15
Step 3: Unpack the new build.....	15
Step 4: Run the upgrade	15
Step 5: Verify the upgrade.....	15

Creating New Server	15
Step 1: Complete a brand new install	16
Step 2: Validate the new server.....	16
Step 3: Change DNS entries	16
Step 4: Turn off old WHS server.....	16
Configuring Workshare Hybrid Storage.....	16
Creating Access Credentials	17
Creating Buckets	19
Purging Deleted Files	22
Automatic purge	22
Statistics.....	23
Error Log	23
Configure Workshare.....	23
Appendix A: Advanced Installation.....	25
Appendix B: Troubleshooting.....	26
What errors logged in the “Errors” page require intervention?	26
What are the typical issues that appear on the “Status” page?	27

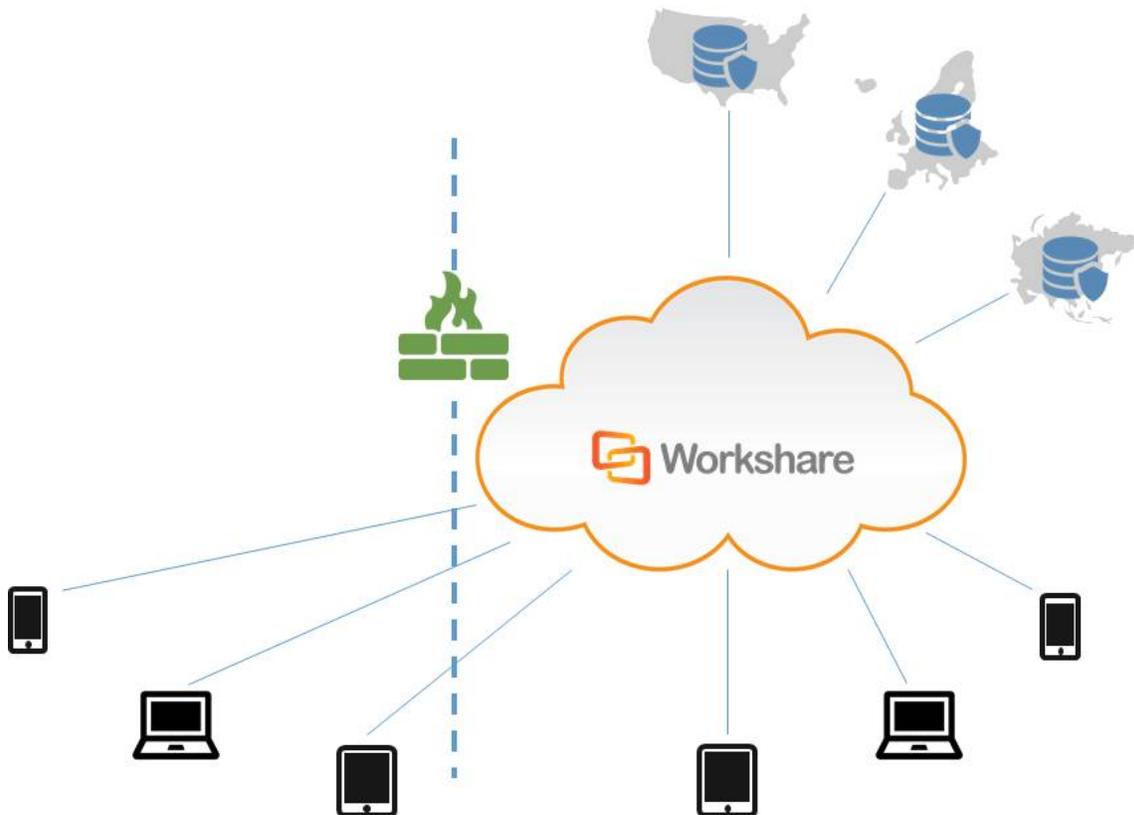
Introduction

Workshare customers can choose between two data storage deployments – Workshare cloud and hybrid cloud.

With a secure Workshare cloud deployment, you can choose a specific data center location provided by Workshare from several locations in the US, South America, Europe and Asia/Pacific. With this option, the jurisdiction under which data falls can be configured to match your requirements.

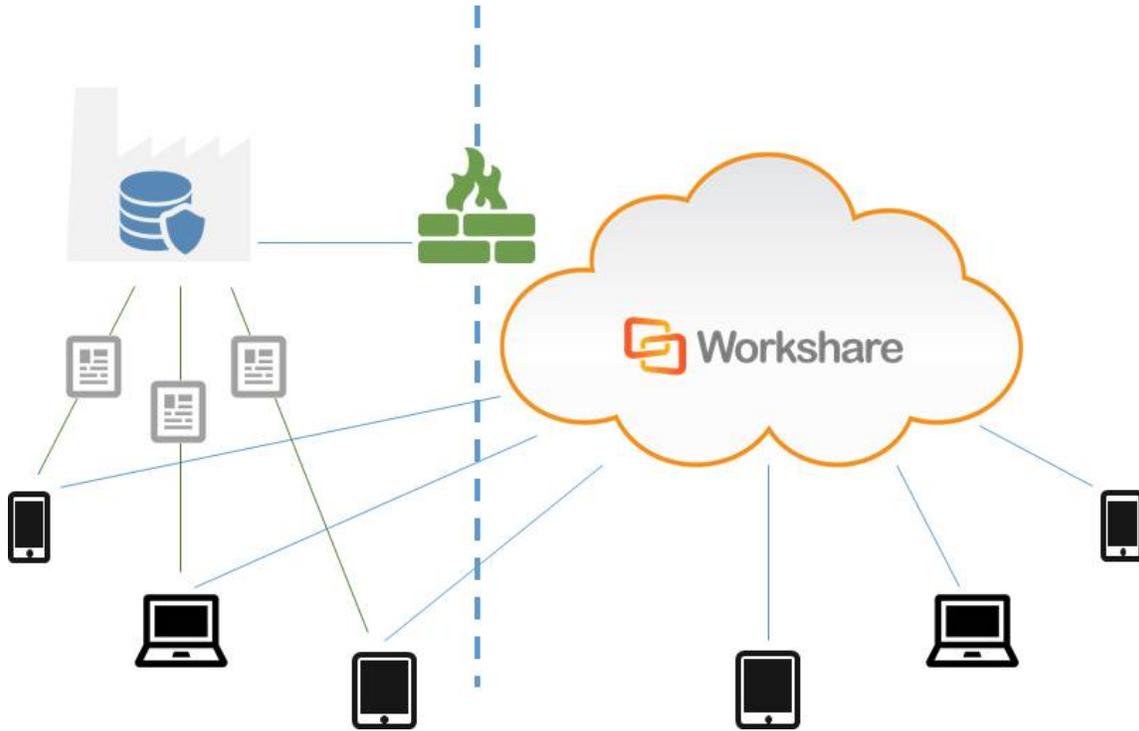
Alternatively, with a hybrid cloud deployment, you can use your own data center that's controlled and managed by your internal IT department. This option provides customers – who already operate or outsource a data center – with their own storage for files. Application and database (profiles, comments and activities' audit trails) are provisioned inside the Workshare cloud; without the context of the documents, this data is essentially obfuscated.

Secure Workshare cloud deployment



With the secure cloud deployment, you can choose a specific US, EMEA or APAC jurisdiction.

Hybrid cloud deployment



With the hybrid cloud deployment, files are stored and controlled by IT behind the organization's firewall or in its own outsourced data center.

This document describes the architecture and set up of the hybrid cloud deployment; no set up is required for Workshare cloud deployment.

Note: With either option, users access Workshare in the same ways and see the same user interface.

Environment Requirements

The Workshare Hybrid Storage (WHS) product provides a robust, performant and secure option for customers who want to store their file content on their premises. WHS builds on trusted technologies such as Microsoft Windows Server, IIS, and Microsoft SQL Server. File content data can be stored in any storage medium that is mounted as a drive or network share on the Windows Server system. WHS also uses an SQL database located within your datacenter to store access control and metadata information about the files it stores.

The recommended system requirements are as follows:

CPU	64-bit architecture-based computer with Intel or AMD processor; 4 CPU cores <i>Note: Two CPU cores is the production minimum and can support typical usage by 500 file sharing users. The product can be run with 1 CPU core for testing/evaluation purposes, but this can cause performance issues, particularly if the SQL database is on the same machine.</i>
Memory	8GB RAM
Storage	1GB free disk space for the application server installation - not for the storage
Networking	Gigabit Ethernet Controller
Supported operating systems	Windows Server 2012 R2, Windows Server 2016
SQL database	SQL Server 2012 or newer

Note: You should ensure that your configuration of IIS meets security standards and best practices. For example, disabling TLS 1.0, using strong cyphers, and so on.

Application Server

WHS can run with a single application server or with multiple application servers (for redundancy or performance) grouped behind a load balancing appliance or software.

Application server instances may be run as physical or virtual machines, but in either case a production application server should have at least 4 cores and 8GB of memory available to it. Application servers do not require a large amount of disk space unless local disks are being used for file content storage (not recommended for production environments).

File Content Storage

WHS requires a folder or drive to store file content data. There are no restrictions on the type of storage that is used for this purpose as long as it can be presented to WHS as a folder or drive (including network shared drives). In the case where multiple application servers are being used, all application servers must access the same shared file content storage folder.

Consideration should be given to the available space and data transfer rate available in the file content storage folder to avoid this becoming a bottleneck for application performance.

Databases

WHS requires two SQL databases, a main database storing file metadata and security information and an errors database which is used to record any errors encountered by the application to allow for problem diagnosis.

WHS service



Network Environment

The WHS server must be accessible from both the internal corporate network and the internet over port 443 (HTTPS). Alternatively, if the WHS server(s) is behind a load balancer or reverse proxy, that proxy/load balancer must be available both internally and externally over port 443.

The WHS server must be given a DNS name (for example `hybridstorage.example.com`) and must be available via that DNS name both internally and externally. The WHS server must present a valid SSL certificate for its DNS name when accessed over HTTPS as it will receive requests from both client applications and browsers and from Workshare application servers over HTTPS. Self-signed certificates will not work. Certificates issued by niche Certificate Authorities may not work. Workshare recommends obtaining a certificate from a reputable CA.

For optimal performance you may wish to ensure that the DNS resolution for your WHS server resolves to its internal IP address for clients within your corporate network, ensuring that they will be able to download content over the local area network.

Considerations for Production/Testing Environments

In your production environment:

Important:

WHS is purely an application server, which consumes storage and database resources. While it is optimized for request throughput and designed for robustness, it does not include any functionality to ensure the redundancy or availability of the data sources it connects to; nor does it include any functionality to perform backups of the underlying data stores.

In a production environment it is absolutely vital to ensure that the databases and file content store are backed up regularly. In many cases it will be possible to do this without excessive effort by utilizing resources that already back up – for instance storing the file content folder on a file server that has a backup schedule or creating the databases on an existing SQL server that has backups configured.

Availability concerns can be addressed by running multiple instances of WHS behind a load balancer to allow for automatic failover if an application instance goes down. For this approach to provide a meaningful boost to availability, the storage and database resources must also have redundancy built in (for instance using a SQL server failover cluster for database storage).

In an evaluation/testing environment:

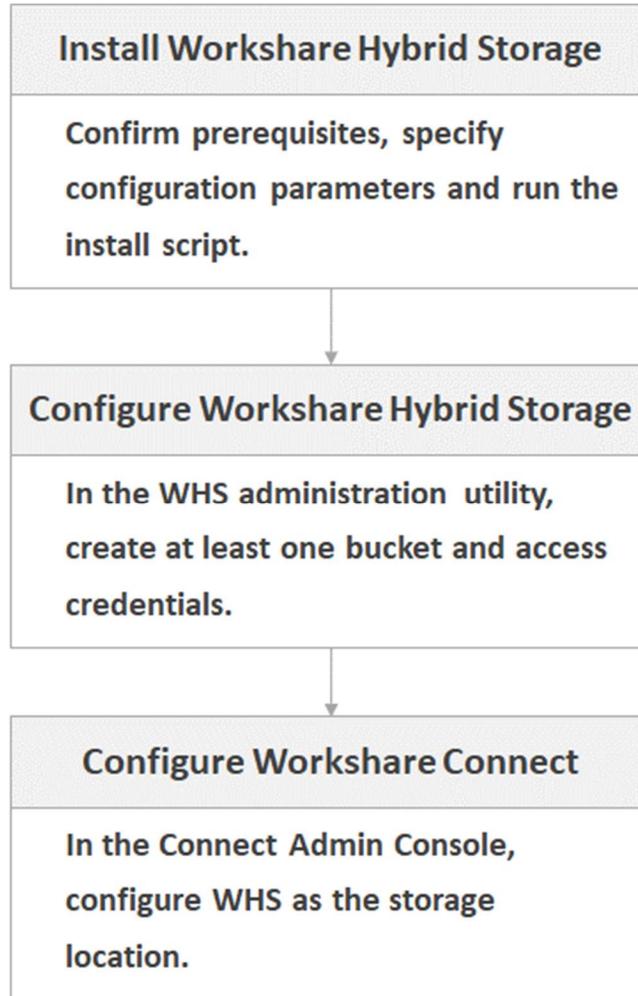
WHS can be run on a single server for evaluation/testing purposes, with database storage provided by a local instance of Microsoft SQL Server Express Edition and file content being stored in a folder on a local hard disk. A valid SSL certificate, DNS name and external access on port 443 for HTTPS will still be required to successfully configure the WHS server for use with Workshare.

Important: *An evaluation or testing environment configured on a single machine should not be promoted to production use, as it is essential to ensure proper backups are in place for any production deployment.*

Once you are ready to use the WHS in production, you must follow the enable production mode steps. It is important to read and understand the statements you verify when enabling production mode in order to validate your entitlement to technical support.

Setup Overview

Deploying and setting up the WHS solution involves the following steps:



Evaluation Mode and Production Mode

WHS has two modes of operation – evaluation mode and production mode. A freshly installed server begins life in evaluation mode. It is fully functional but has a big orange warning on the admin screen that it is in evaluation mode.

Evaluation mode servers should be used for testing and evaluation and must not be used for storing 'production' files. Our definition of production files is 'anything that you care about enough to try to recover if it gets lost or deleted'.

Production mode servers can be used to store production files. Before enabling production mode, you must follow the 'Enable Production Mode' link in the Workshare admin UI and confirm that you have implemented and understood the list of requirements for a production mode server. For example, that you understand WHS is designed to run on top of services that have redundant capacity and that are backed up. The date, user name and list of statements that you have confirmed are stored in the database.

Deploying Workshare Hybrid Storage

The Workshare Hybrid Storage product is deployed using a PowerShell script. A small number of configuration parameters in a configuration file can be modified to cater for most deployment scenarios.

Prerequisites

Before any deployment, the following steps must be completed:

- Select a domain name for the server – for example, **hybridstorage.mydomain.com**.
- Obtain an SSL certificate in PFX format for this domain (or a wildcard certificate for *. **mydomain.com**). Place this on the target machine.
- Configure DNS records so that **hybridstorage.mydomain.com** resolves correctly for both internal and external users.
- Configure any corporate firewall to allow HTTPS requests to reach the server either directly or via a load balancer or reverse proxy.

Installation Process

Deployment should begin with a clean but fully up-to-date install of Windows Server, ideally with all service packs and updates installed.

Step 1: Obtain and unpack the Workshare.HybridStorage- <VersionNumber>.zip file

This can be unpacked to any location on the target system. Once unpacked you will find the 'SetupServer.ps1' PowerShell script among the unpacked files – this is the installation script. Additionally you will find a PowerShell script called 'Configuration.ps1' – this contains all the configuration variables that may need to be changed to customize the installation.

Note: Before unzipping the downloaded zip file, ensure it is unblocked. Right-click the zip file and select **Properties**; select the **Unblock** checkbox and click **Apply**; click **OK** to close.

Step 2: Edit the 'Configuration.ps1' file

Make appropriate changes in the configuration file – see options and their definitions in the *Script Configuration Options* section.

Step 3: Run the 'SetupServer.ps1' file

Right click the 'SetupServer.ps1' file and select 'Run with PowerShell'. As the installation requires administrative permissions, you may be shown a User Account Control prompt, which you must allow. You will also need to accept the end user license agreement.

When running the script for the first time, you may be prompted with the following message:

```
Execution Policy Change
The execution policy helps protect you from scripts that you
do not trust. Changing the execution policy might expose you
to the security risks described in the about_
Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170.
Do you want to change the execution policy? [Y] Yes [N] No
[S] Suspend [?] Help (default is "Y")
```

You must answer 'Y' to this prompt to allow the installation script to run.

Script Configuration Options

All of these configuration variables can be found and altered in the 'Configuration.ps1' file.

Web Site Configuration	
<code>\$WebSiteName</code>	The name of the web site to create or use in IIS.
<code>\$AppPoolName</code>	The name of the application pool to create or use.
<code>\$WebSiteInstallPath</code>	The location on disk to install the WHS web site executable files.
<code>\$ErrorLogRetentionTimeDays</code>	The length of time to keep error reports in the error log database. The default setting is 14 days.

In most scenarios these variables can be left at their default values.

Application Pool Configuration	
<code>\$AppPoolUserName</code>	The username of the windows login to be used to run the web site.
<code>\$AppPoolPassword</code>	The password of the windows login to be used to run the web site.

If the `$AppPoolUserName` configuration option is left blank then the default identity will be used to run the web site (“IIS AppPool\`$AppPoolName`”). The application pool user may need to be changed from the default under the following circumstances:

- Accessing SQL databases on a different machine using ‘integrated’ authentication.
- Accessing a file content storage folder on a network share.

HTTPS Configuration	
<code>\$CertificateFilePath</code>	The full file path to the HTTPS certificate (PFX) file to be used.
<code>\$CertificatePassword</code>	The password used to secure the PFX certificate file.

These configuration options need to be set for all installations (except in the case that incoming HTTPS requests will be handled at a separate reverse-proxy server which will forward the requests over HTTP to the WHS server). Note that you will not be able to configure WHS as a storage location in Workshare if the HTTPS configuration is incorrect or incomplete.

SQL Configuration	
<code>\$SqlServer</code>	The server name and instance name of the SQL server to connect to.
<code>\$StorageDBName</code>	The name of the database to use (or create) for the primary service data store.
<code>\$ErrorsDBName</code>	The name of the database to use (or create) for the error data store.
<code>\$DatabaseUserName</code>	The user name to use when connecting to the SQL server using SQL authentication. Integrated authentication mode will be used when <code>\$DatabaseUserName</code> is left blank.
<code>\$DatabasePassword</code>	The password to use when connecting to the SQL server using SQL authentication.
<code>\$CreateDatabases</code>	If set to true then the installation script will attempt to create, initialize and assign permissions to the required databases.

The `$SqlServer` configuration option must be changed for any production deployments - it must reference an SQL Server instance with appropriate resilience and an operational backup strategy.

If the `$SqlServer` configuration option is left at the default value of “.\SQLEXPRESS”, the installation script will install Microsoft SQL Server 2014 Express Edition on the target system if it is not already installed. This option is suitable for testing and evaluation deployments.

The creation and provision of the databases (`$CreateDatabases=$true`) will only work if:

- SQL authentication is in use (ie `$DatabaseUserName` and `$DatabasePassword` have been set) and the credentials in use have permission to create databases
- or
- The user running the installation script has permission to create, modify and assign permissions to databases on the target SQL server

Note: If (`$CreateDatabases=$true`) and integrated authentication is being used, then the Windows user that will be used for the Application pool needs to exist on the SQL server. To ensure this, the setup will automatically determine the Windows login used to access the database and create that user on the SQL server. If the user already exists on the SQL server, it may be deleted and recreated by this process.

File Content Storage Configuration

<code>\$BlobStoragePath</code>	The path of the folder where file content data is to be stored
--------------------------------	--

This configuration option must be set correctly for all production deployments – it must point to a file system (either network or local) with sufficient capacity for projected usage and a valid backup strategy.

While this option may point to a network shared location, special care must be taken if using a path on a mapped network drive, since Windows maps network drivers on a per-user basis. This means that if the installing administrative user creates a drive mapping from z:\ to \\fileserver\share, that drive mapping will not be visible to the web application running under a different identity.

Deploying an Evaluation/Testing Environment

For evaluation and testing, the only details that need updating in the configuration script are the HTTPS certificate related options (`$CertificateFilePath` and `$CertificatePassword`). All other options can be left as default, which will mean that a local instance of SQL Server Express Edition will be used for database storage and a folder will be created at 'c:\blobs' for file content storage.

Deploying a Production Environment

For a production environment the following conditions must be ensured:

- That the SQL databases used by WHS – particularly the ‘storage’ database are regularly backed up.
- That the file content storage path used by WHS to store file content is regularly backed up.

If a high availability configuration is desired then both of these resources should be considered critical and should be implemented in a resilient and highly available manner.

In general, the above considerations mean that for a production environment, the database and file content storage folder will not be located on the servers running the WHS web application. This has implications for the configuration of the WHS web service, namely that the default Application Pool identity will probably not be able to gain access to either resource through integrated windows authentication.

The preferred solution is to create a domain user account to be used to run the WHS web service and to grant access to this account to the database and file storage resources. For example in the ‘Configuration.ps1’ file:

```
$AppPoolUserName="mydomain\hybridstorage"  
$AppPoolPassword("<password>")
```

Upgrading Workshare Hybrid Storage

When you want to install a new version of the WHS software, you can either update your existing WHS server or set up a brand new WHS server and transfer traffic to it.

Whichever method you choose, you should first:

- Backup your SQL database
- Backup your file storage

Note: *It is very important that you perform these backups prior to an upgrade.*

Upgrading Existing Server

When you perform an in-place upgrade, you must plan for downtime. The hybrid storage service will be unavailable during the upgrade procedure and although the upgrade should not take long, you must make allowance for this. If you want to avoid downtime altogether, you may want to consider [creating a new server](#).

Step 1: Back up install folder

Copy, not move, the WHS install folder (default C:\hybridstorage) to another location. This is to ensure a rollback strategy should there be any problems with the upgrade.

Step 2: Confirm configuration settings

Your previous WHS installation will have made a copy of the Configuration.ps1 file in the WHS install folder (default C:\hybridstorage) called **InstalledConfiguration.ps1**. Open this configuration file in a text editor and confirm that the settings saved from the previous installation are still correct. For example, the database name, the file storage location.

Make any necessary changes in **InstalledConfiguration.ps1** and save the file.

Warning: *If InstalledConfiguration.ps1 is not an accurate reflection of your settings, the upgrade could fail.*

Step 3: Unpack the new build

This can be unpacked to any location on the target system. Once unpacked, find the **Upgrade.ps1** file.

Step 4: Run the upgrade

Run the PowerShell script **Upgrade.ps1**. Ensure it completes without errors.

Step 5: Verify the upgrade

Check the functionality of WHS by uploading and downloading files to check it is working as expected.

If there are any problems with the upgrade, roll back to your previously installed version by copying the previous installation folder (copied in step 1) to the install location. Contact Workshare Customer Support for further help.

Creating New Server

To avoid any downtime during an upgrade, you can install the new version of WHS on a fresh server that communicates to the same database and file server as the previous version. Once the new server is up and running correctly, you can switch off the old version.

Note: *This upgrade method will **only** work if your database is accessed remotely and your file store is on a network share.*

Step 1: Complete a brand new install

Follow the full install procedure described in the [Installation Process](#).

Note: You can look in the configuration file (*InstalledConfiguration.ps1*) of your previous WHS install to gather the settings you require for installation.

Step 2: Validate the new server

Check the new server is functioning correctly – you can do this via the WHS admin console or using an Amazon S3 compatible client like CloudBerry Explorer.

Note: You may need to edit the hosts file at: *c:\windows\system32\drivers\etc\hosts* on the machine from which you are running tests to ensure that the DNS name used for the old server points to the IP address of the new server on that machine only. Remember to undo changes to the hosts file once testing is complete.

Step 3: Change DNS entries

Ensure that both internal and external DNS entries for the hybrid server are both updated.

Step 4: Turn off old WHS server

Once DNS is fully propagated, you can turn off the old server. Check the server logs to ensure that no new requests are being made to the old server and then power the old server down.

Configuring Workshare Hybrid Storage

The WHS install makes an administrative console available over http from the machine itself. Login is by Windows login credentials for the machine on which the service is running and is restricted to members of the 'Administrators' Windows group.

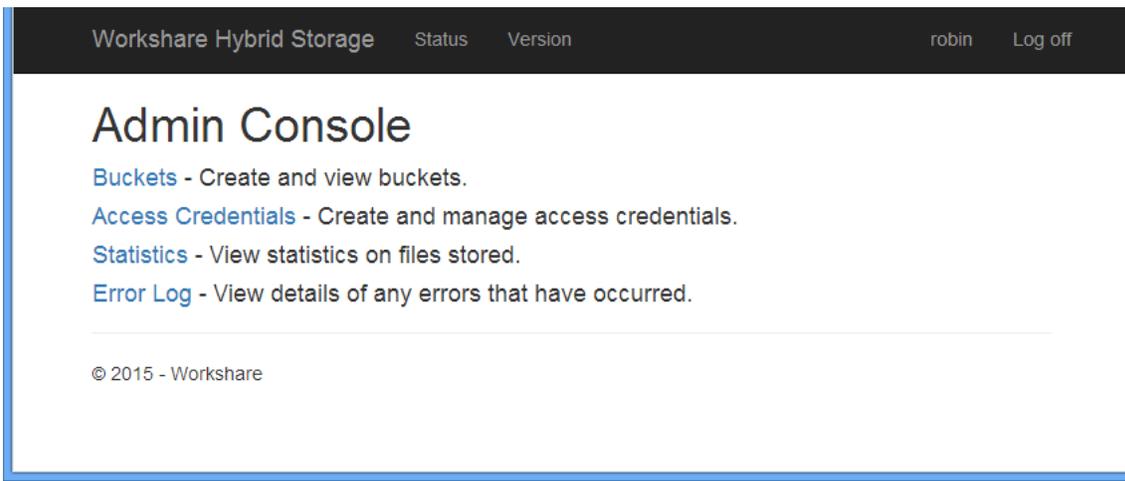
For security reasons, the admin console is only available by default via a browser on the WHS server. If you want to make it available from other devices, you'll need to change the following parameter in appSettings in the web.config file.

```
<add key="AllowRemoteAdminLogin" value="false"/>
```

If this is set to `True`, the admin console will also be available at the URL `https://<servername>/storage.admin`.

You will need to use the WHS administrative console to create at least one set of credentials and at least one bucket in order to register your WHS server with Workshare.

Once logged in, there are four areas available in the WHS administrative console – Buckets, Access Credentials, Statistics and Error Log.



Two pages are available to non-logged-in users –<https://<servername>/storage.admin/healthcheck> and <https://<servername>/storage.admin/version>. These provide an indication of WHS health and version information for the WHS software respectively. The health check URL is suitable for use as a test URL by which a load balancing device can check that an instance is ready to receive requests. More detailed information can be found by a logged in user by clicking the **Status** and **Version** links in the navigation bar of the WHS administrative console.

Creating Access Credentials

Credentials are used to authenticate requests to WHS to upload or download file content. Credentials consist of two elements – the Access Key (which is 20 characters long, starts with a 'W' and contains upper case letters and numbers) and a Secret Key (which is 40 characters long and contains upper and lower case letters, numbers and some other characters).

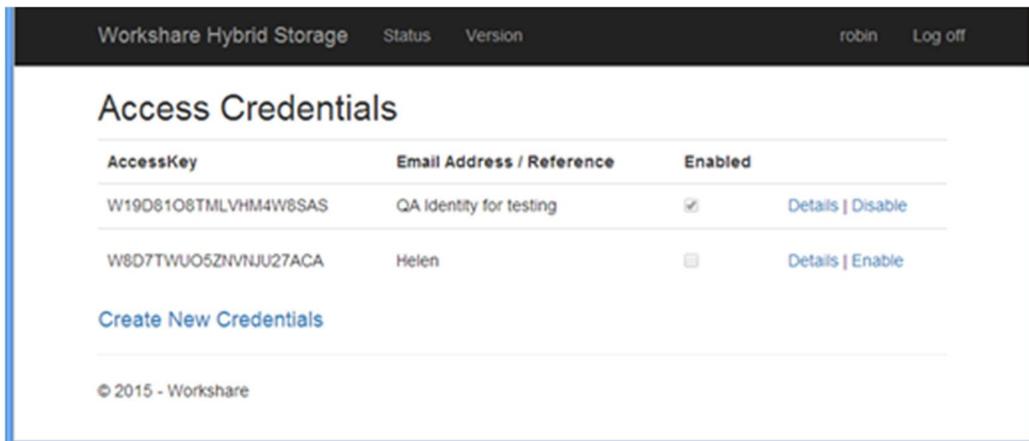
Knowledge of the Access Key and corresponding Secret Key allows a cryptographic signature to be created to authorize any request for file content in any bucket to which the credentials have been granted permission.

You will need to create at least one set of credentials to be able to create any buckets (buckets need to have an owner). You will need to have your Access Key and Secret Key available when configuring a custom storage location on Workshare to use your WHS server. The Workshare servers will use your credentials to create appropriate signed requests against the WHS server to allow authenticated users of Workshare to download and/or view file content.

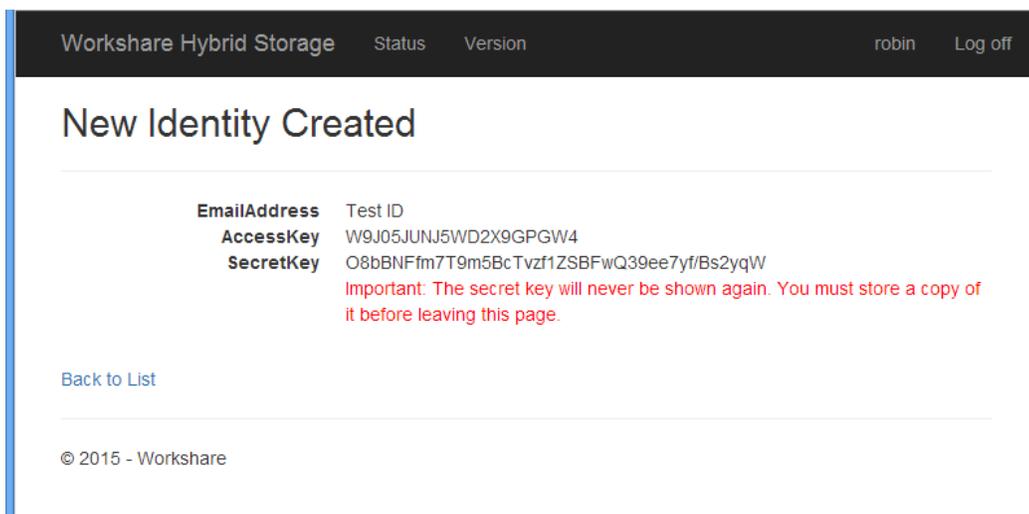
When creating a new set of access credentials, it is important to take a copy of the generated Secret Key, as this will only be shown during the credential creation procedure and cannot be shown again. Note that the credential Secret Key is stored in an encrypted form in the SQL database.

To create access credentials:

1. Click **Access Credentials** in the WHS administrative console.

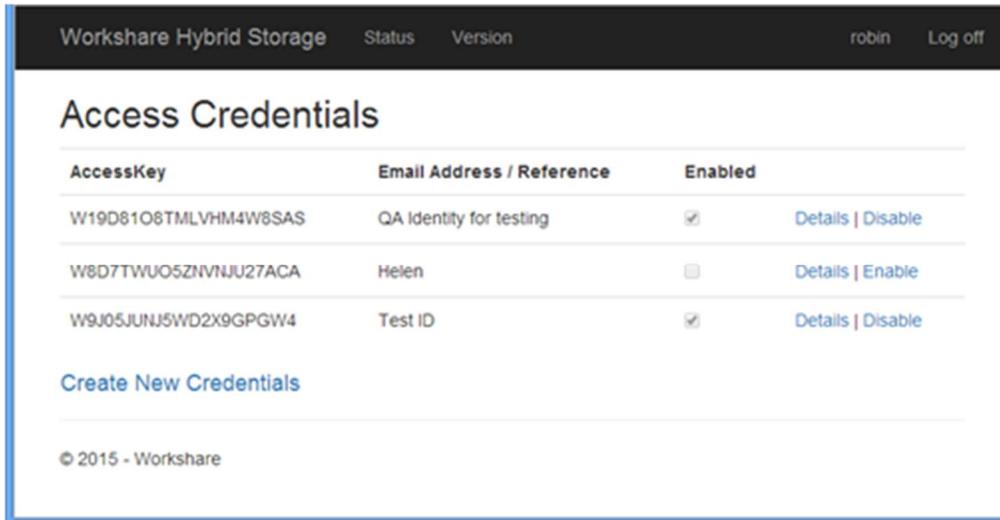


2. Click **Create New Credentials**.
3. Enter a name for the credentials and click **Create**. An Access Key and Secret Key are assigned to the new credentials.



4. Make a note of the Secret Key as it will never be shown again and you need it later when configuring Workshare.

5. Click **Back to List**.



AccessKey	Email Address / Reference	Enabled	
W19D81O8TMLVHM4W8SAS	QA Identity for testing	<input checked="" type="checkbox"/>	Details Disable
W8D7TWUO5ZNVNJU27ACA	Helen	<input type="checkbox"/>	Details Enable
W9J05JUNJ5WD2X9GPGW4	Test ID	<input checked="" type="checkbox"/>	Details Disable

[Create New Credentials](#)

© 2015 - Workshare

The credentials you have just created appear in the list and are enabled by default. Credentials cannot be deleted, but may be disabled if preventing access either temporarily or permanently is required.

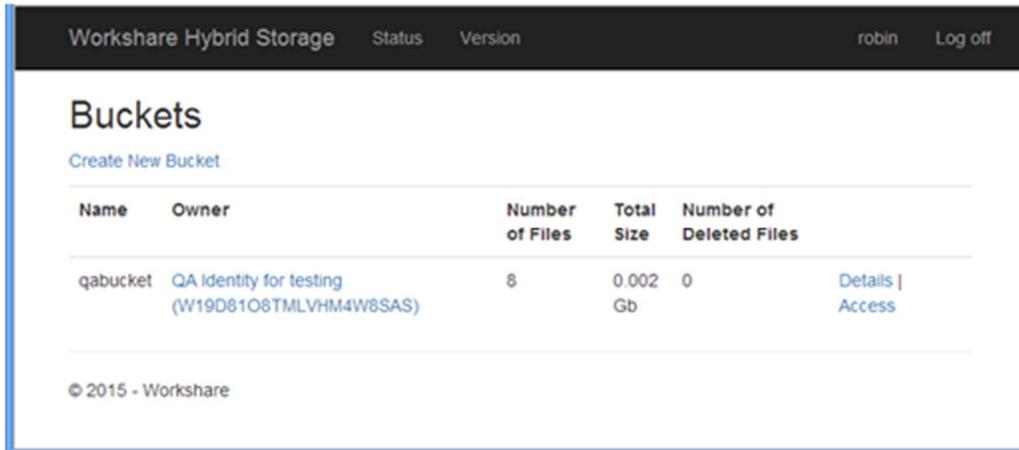
Creating Buckets

Buckets are the containers in which WHS stores files. Each bucket can store many hundreds of thousands – or even millions – of files if necessary. Only one bucket is needed for WHS although the option to create more is available.

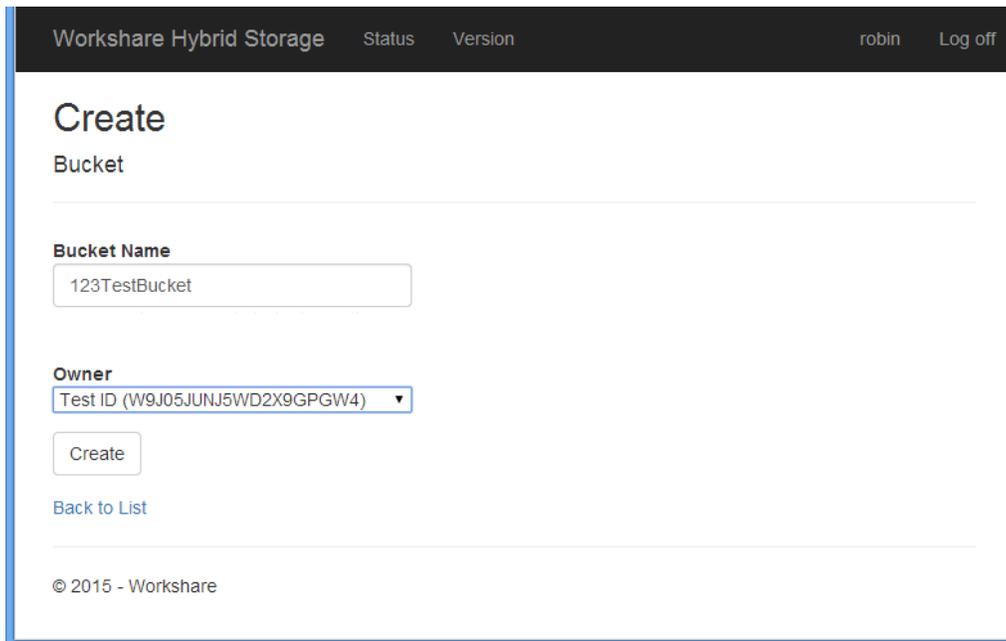
Bucket names must be at least 3 characters long and are restricted to the letters A-Z, a-z, the digits 0-9 and the '-' and '.' characters. Access to buckets is by Access Keys and you will not be able to create a bucket until you have created at least one Access Key (by creating access credentials).

To create a bucket:

1. Click **Buckets** in the WHS administrative console.



2. Click **Create New Bucket**.
3. Enter a name for the bucket and select an owner for the bucket. The list includes all the access credentials you have created, by name and Access Key.



4. Click **Create**.

Workshare Hybrid Storage Status Version robin Log off

Bucket Details

Name	123TestBucket
Owner	Test ID (W9J05JUNJ5WD2X9GPGW4)
Number of Files	0
Total Size	0.000 Gb
Number of Deleted Files	0
Deleted File Size	0.000 Gb

[Back to List](#)

© 2015 - Workshare

5. Click **Back to List**.

Workshare Hybrid Storage Status Version robin Log off

Buckets

[Create New Bucket](#)

Name	Owner	Number of Files	Total Size	Number of Deleted Files	
qabucket	QA Identity for testing (W19D81O8TMLVHM4W8SAS)	8	0.002 Gb	0	Details Access Purge Deleted
123TestBucket	Test ID (W9J05JUNJ5WD2X9GPGW4)	0	0.000 Gb	0	Details Access Delete

© 2015 - Workshare

The bucket you have just created appears in the list and is enabled by default.

The identity whose Access Key is used to create a bucket will become the owner of the bucket and will always have access to that bucket. Other identities can be granted access, or have access removed, via the **Access** link.

Only empty buckets may be deleted – via the **Delete** link – this avoids unintentional loss of data. Additionally, WHS delays deletion of items within a bucket until an administrative user activates the 'Purge Deleted' link which appears for buckets that contain deleted files.

Purging Deleted Files

When files are deleted by a user in Workshare Connect, they are moved to the Recycle bin. When the user empties the Recycle bin, the files get flagged for deletion in the Connect database. Connect will send a message to WHS to delete the file. WHS sets a flag saying the file has been deleted and the file counts as one of the deleted files in the bucket. The admin must purge the deleted files so they are fully deleted and the content is removed from disc.

To purge deleted files:

Click **Purge Deleted** to the right of the bucket.

The screenshot shows the Workshare Hybrid Storage admin interface. At the top, there is a navigation bar with 'Workshare Hybrid Storage', 'Status', and 'Version' on the left, and 'robin' and 'Log off' on the right. The main content area is titled 'Purge Deleted Files' and contains the question 'Are you sure you want to purge the deleted files in this bucket?'. Below this is a table with the following data:

Name	Test Bucket
Owner	test (WRPLT9XF0XKXA7RGFOF1)
Number of Files	5258
Total Size	0.047 Gb
Number of Deleted Files	638
Deleted File Size	0.007 Gb

At the bottom of the dialog, there are two buttons: 'Purge' and 'Back to List'. The footer of the page reads '© 2019 Workshare Ltd'.

Click **Purge**. The files that have the deleted flag set on them in the database are now fully deleted and the content is removed from disc.

Automatic purge

Deleted files can be automatically purged – by default they are not – by modifying a parameter in the web.config file (located in the Install folder).

Locate the following parameter in appSettings in the web.config file.

```
<add key=" AutoPurgeDeletedFilesAfter " value="-1"/>
```

If this is set to zero or greater then deleted files will be automatically purged that number of days after their deletion.

If set to -1 or any other negative value then auto-purge is disabled and purging of deleted files must happen manually from the admin console.

Statistics

Clicking **Statistics** in the WHS administrative console displays the statistics page. This provides a summary of the total amount of data stored by WHS and a breakdown of the storage by buckets.

Error Log

Clicking **Error Log** in the WHS administrative console displays the error log page. This provides a list of all failed web requests against the WHS server. This information is only needed when attempting to diagnose any bugs or issues affecting WHS.

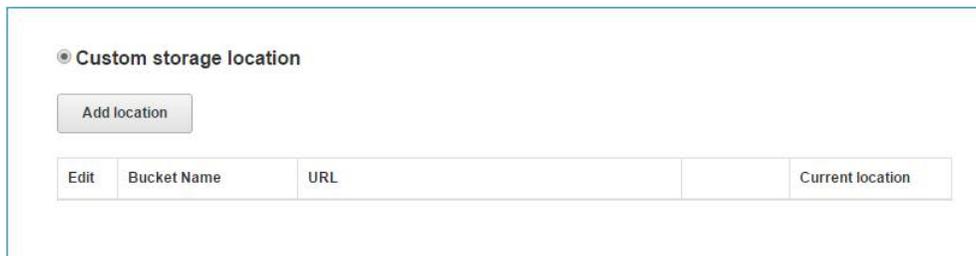
It is entirely normal for entries to be added to this log during the correct operation of WHS – for example failures to login to the administrative console or random unauthenticated web requests made of the WHS server would result in entries in the error log being created. The presence of entries in the error log does not, by itself, indicate that WHS is operating incorrectly or that any corrective action needs to be taken.

Configure Workshare

Once you have deployed and configured WHS, you can configure WHS as a storage location in Workshare.

To change your data storage location in Workshare:

1. Log into your Workshare account on my.workshare.com.
2. Click your user name and select **Admin Console**.
3. Select the **Data Management** tab.
4. Ensure **Storage** is selected in the left menu.
5. Select **Custom storage location**.

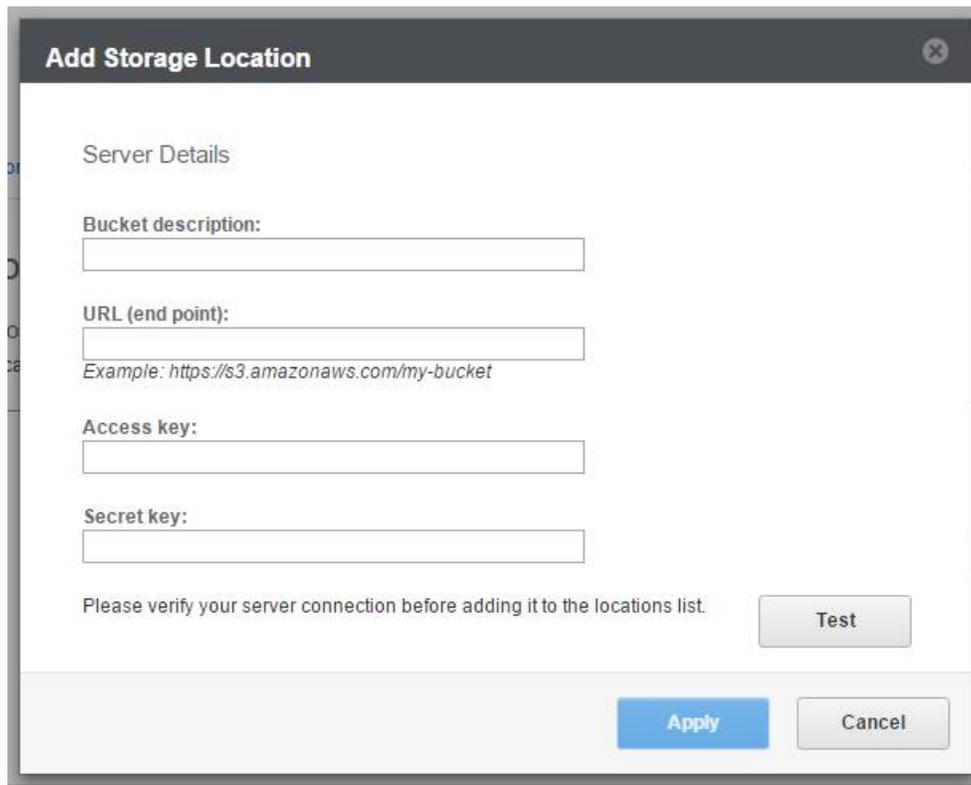


● Custom storage location

Add location

Edit	Bucket Name	URL	Current location
------	-------------	-----	------------------

6. Click **Add location**.



Add Storage Location

Server Details

Bucket description:

URL (end point):

Example: https://s3.amazonaws.com/my-bucket

Access key:

Secret key:

Please verify your server connection before adding it to the locations list.

Test

Apply Cancel

7. Enter a description of the bucket, the URL, and the access key and secret key that you generated earlier.
8. Click **Test** to verify the server connection.
9. Click **Apply**.

Appendix A: Advanced Installation

If you are unable to use the automatic database creation option in the install script (`$CreateDatabases=$true`) then you will need to manually create the databases required by the WHS server before installing. The procedure for manually creating and configuring the databases is as follows.

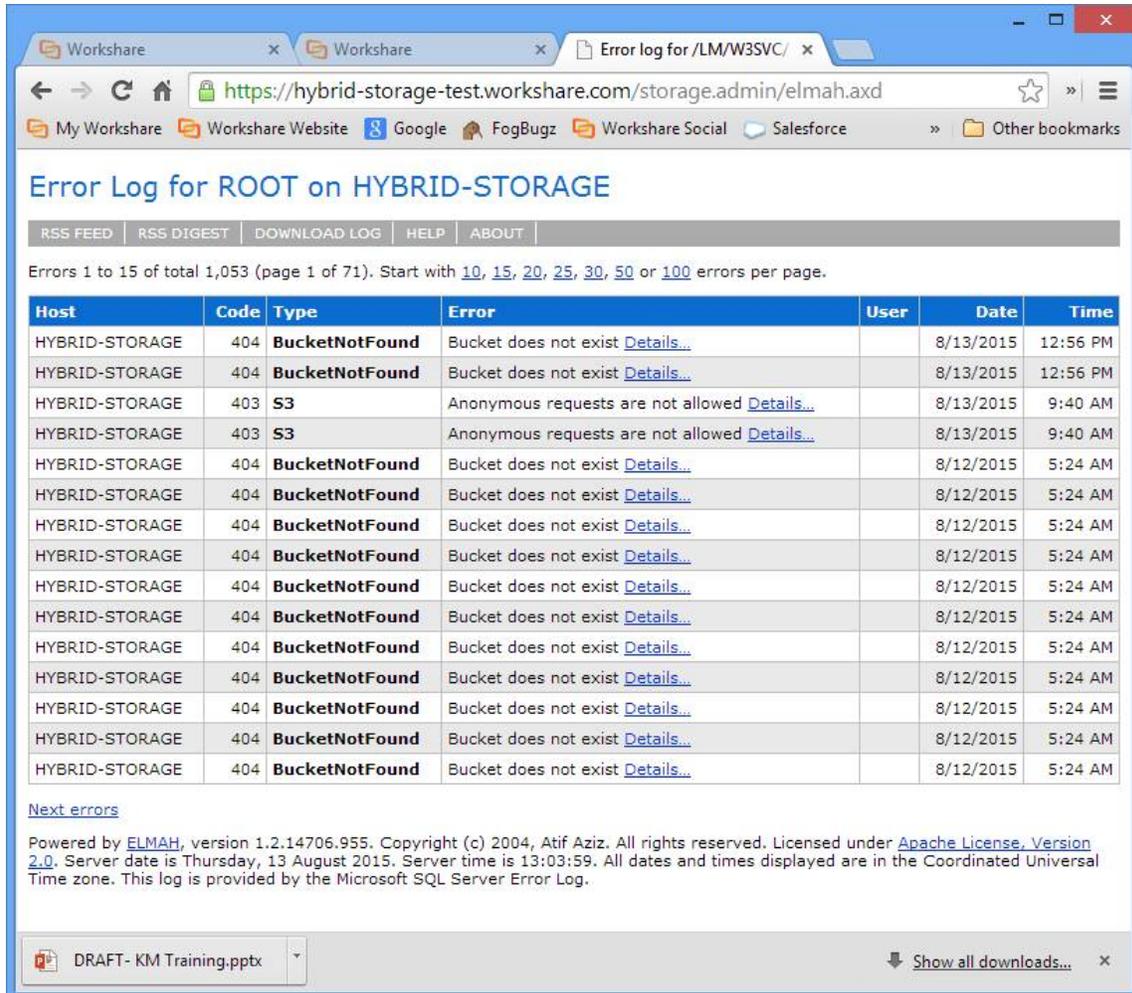
To manually configure the WHS databases:

1. Create two empty databases on the database server – one for the storage metadata and one for the errors database.
2. Decide which authentication method you are going to use to connect to the database – SQL server username/password authentication or Windows integrated authentication.
 - For integrated authentication, grant access to each database (in the role 'db_owner') to the identity under which the web service application pool will be running (`$AppPoolUserName`)
 - For SQL server authentication, grant access to each database (in the role 'db_owner') to the user which will be used to connect to the database (`$DatabaseUserName`)
3. Populate the required table structure and stored procedures into the errors database by running the 'ELMAH-1.2-db-SQLServer.sql' script against the errors database. (Note that no pre-configuration is required for the storage database).

Appendix B: Troubleshooting

What errors logged in the “Errors” page require intervention?

Clicking **Error Log** in the WHS administrative console displays a detailed error log:



The screenshot shows a web browser window displaying the 'Error Log for ROOT on HYBRID-STORAGE' page. The page includes a navigation bar with links for RSS FEED, RSS DIGEST, DOWNLOAD LOG, HELP, and ABOUT. Below the navigation bar, there is a message indicating 'Errors 1 to 15 of total 1,053 (page 1 of 71). Start with 10, 15, 20, 25, 30, 50 or 100 errors per page.' The main content is a table of error logs.

Host	Code	Type	Error	User	Date	Time
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/13/2015	12:56 PM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/13/2015	12:56 PM
HYBRID-STORAGE	403	S3	Anonymous requests are not allowed Details...		8/13/2015	9:40 AM
HYBRID-STORAGE	403	S3	Anonymous requests are not allowed Details...		8/13/2015	9:40 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM
HYBRID-STORAGE	404	BucketNotFound	Bucket does not exist Details...		8/12/2015	5:24 AM

Next errors

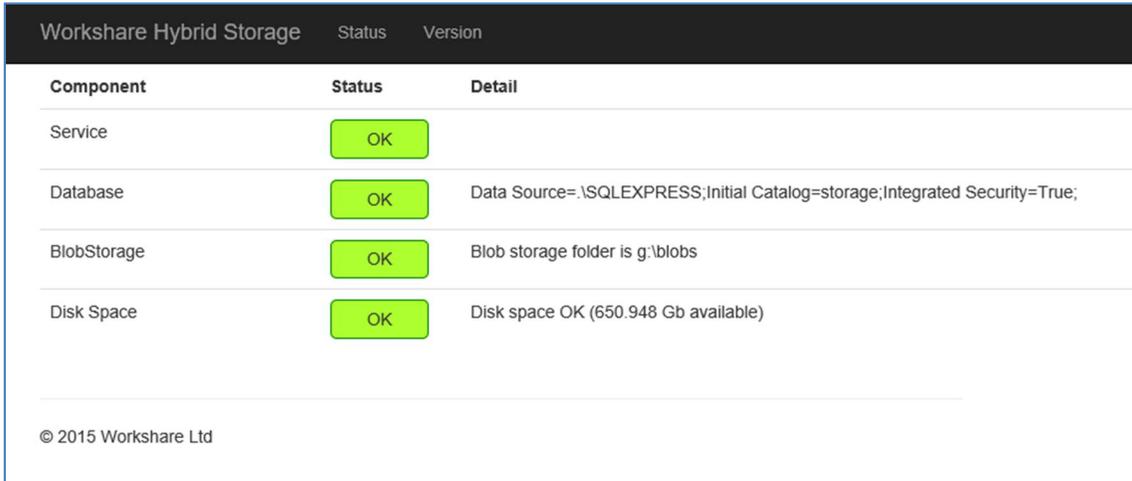
Powered by **ELMAH**, version 1.2.14706.955. Copyright (c) 2004, Atif Aziz. All rights reserved. Licensed under [Apache License, Version 2.0](#). Server date is Thursday, 13 August 2015. Server time is 13:03:59. All dates and times displayed are in the Coordinated Universal Time zone. This log is provided by the Microsoft SQL Server Error Log.

In general, do not use this error log for monitoring purposes in order to spot where intervention may be necessary. This error log is more useful for diagnosing issues so that if a problem occurs you can use the error log to try and find the cause of the problem.

Many 'error' reports are actually just failed HTTP requests which do not indicate an issue or bug in the software. For example, some request URLs may have a time limit within which they must be used - re-use of the request URL. After the time limit has expired (perhaps caused by the user opening their laptop and refreshing an old browser tab) it would get logged into the error database but is not an indication of a flaw in the software.

What are the typical issues that appear on the “Status” page?

Clicking the **Status** link in the navigation bar of the WHS administrative console displays the status page:



Workshare Hybrid Storage		
	Status	Version
Component	Status	Detail
Service	OK	
Database	OK	Data Source=.\SQLEXPRESS;Initial Catalog=storage;Integrated Security=True;
BlobStorage	OK	Blob storage folder is g:\blobs
Disk Space	OK	Disk space OK (650.948 Gb available)

© 2015 Workshare Ltd

This provides an indication of WHS health. For example:

- A red light next to **Database** indicates a problem with the connection to the database, for example, if the SQL connection goes down.
- A red light next to **BlobStorage** indicates no communication to the content storage file share.
- A red light next to **Disk Space** indicates available disk space is running low - below 10GB.

 Workshare Ltd.

© 2019. Workshare Ltd. All rights reserved.

Copyright

Workshare Professional and Workshare DeltaView are registered trademarks of Workshare Ltd. Workshare Compare, Workshare Protect, Workshare 3, Workshare DeltaServer, SafetyGain, and the Workshare logo are trademarks of Workshare Ltd. All other trademarks are those of their respective holders.

Trademarked names may appear throughout this guide. Instead of listing these here or inserting numerous trademark symbols, Workshare wishes to state categorically that no infringement of intellectual or other copyright is intended and that trademarks are used only for editorial purposes.

Disclaimer

The authors/publishers of this guide and any associated help material have used their best efforts to ensure accuracy and effectiveness. Due to the continuing nature of software development, it may be necessary to distribute updated help from time to time. The authors would like to assure users of their continued best efforts in supplying the most effective help material possible.

The authors/publishers, however, make no warranty of any kind, expressed or implied, with regard to Workshare programs or help material associated with them, including this guide. The authors/publishers shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the programs or associated help instructions.

For details of Workshare patents, see www.workshare.com/patents

Revisions

Published for Workshare Hybrid Storage: 07/10/19; minor revisions: 06/11/19

Workshare Ltd., 20 Fashion Street, London E1 6PX www.workshare.com