

User manual

WebShare G8

(Version 5.0.0)

User manual

September 10, 2020

Contents

1	About the chapters of this manual	1
2	An introduction to HELIOS WebShare	5
2.1	New WebShare features	6
2.2	Client file transfer and syncing applications included with WebShare	6
2.2.1	WebShare Manager	6
2.2.2	Document Hub	7
2.3	Integration with other HELIOS products	7
3	Installation	9
3.1	Different setups	9
3.1.1	General overview	9
3.1.2	Software firewall (Internet)	10
3.1.3	Hardware firewall (Internet)	11
3.1.4	Hardware firewall (Intranet)	11
3.1.5	Single-server solution	12
3.2	WebShare Web Server installation	13
3.2.1	System requirements	13
3.2.2	Software installation	13
3.2.3	Verifying the installation	14

3.3	WebShare File Server installation	16
3.3.1	System requirements	16
3.3.2	Software installation and licensing	16
3.3.3	Verifying the installation	17
4	Administration	19
4.1	Server Preferences	21
4.2	Quickshare Administration	27
4.3	User Administration	28
4.4	Organize sharepoints	34
4.5	Sharepoint Administration	35
4.6	Accounting	41
4.7	Branding Editor	44
4.7.1	Create and configure brandings	45
4.7.2	Import brandings	53
4.7.3	Brandings and the “style” file	54
4.7.4	Add custom file icons	55
4.7.5	Add custom banner images	55
4.7.6	Banner image URL mapping	55
4.7.7	Add custom banner text	56
4.7.8	Customize brandings via CSS	57
4.7.9	Customize brandings via JavaScript	59
4.7.10	Custom toolbar icons	60
4.7.11	Custom actions icons	61

4.8	Java Server Statistics	61
4.8.1	WebShare Server Information	62
4.8.2	WebShare Java Information	63
4.8.3	WebShare User Statistics	63
4.9	HELIOS Icon Collector	63
4.9.1	Icon Collector (Windows)	64
4.9.2	Icon Collector (OS X)	64
4.9.3	Usage	64
4.10	WebShare URL Share Access	68
4.10.1	Required parameter	70
4.10.2	Login parameters	70
4.10.3	Path parameters	70
4.10.4	Image parameters	71
4.10.5	Response parameter	72
4.10.6	Image only parameters	72
4.10.7	Preview page parameters	73
4.10.8	Examples	74
4.10.9	URL Share Access Helper	75
4.10.10	Security considerations	76
4.11	WebShare catalog presentation	76
4.12	Troubleshooting	79
4.12.1	Limitations	82
5	HELIOS Admin	83

5.1	General remarks	83
5.2	WebShare Server Settings	84
5.3	Sharepoints	88
5.4	WebShare Users	92
5.5	WebShare log file	95
6	Using WebShare	97
6.1	WebShare File Server login	97
6.2	WebShare access keys	100
6.3	Work in a sharepoint	102
6.3.1	The WebShare toolbar	104
6.3.2	Add file comments	117
6.3.3	Note on file access permissions	118
6.3.4	Logout	119
6.4	Image and document previews	120
6.4.1	Previewing images and single document pages	122
6.4.2	Image Editor	124
6.4.3	“Color Info”	128
6.4.4	“Annotations”	130
6.4.5	Previews of multiple-page documents	133
6.4.6	Banner and trailer files per document	136
6.4.7	Preview/proof print settings	137
6.5	Remote Proofing	139
6.6	WebShare Quickshares	140

6.6.1	Create Quickshares	140
6.6.2	Manage your own Quickshares	141
6.6.3	Upload files to a Quickshare	142
6.7	My User Preferences	142
6.8	WebShare file format support	146
6.8.1	Supported upload formats	146
6.8.2	Supported download formats	147
6.9	Supported browsers	147
7	WebShare Web Server	151
7.1	WebShare license information	151
7.2	WebShare Web Server files	152
7.3	Customization/Localization	155
7.3.1	Customizing “*.html” files	156
7.3.2	Customizing “*.wod” files	156
7.3.3	Customizing action scripts	156
7.3.4	Adding additional language localizations	157
7.4	HTTP/SSL support	157
7.4.1	Introduction	157
7.4.2	Background	158
7.4.3	Import an exiting certificate	159
7.4.4	Request and import a new certificate from a CA	160
7.4.5	Create a certificate using an online CA (RFC 8555)	161

7.4.6	Create a self-signed certificate	162
7.5	wskeytool	162
7.5.1	Completion	177
7.5.2	Q & A	178
7.5.3	Known issues	178
7.6	Preferences	179
7.6.1	WOSTarter preference keys	187
8	WebShare File Server	189
8.1	User configuration file	189
8.2	WebShare user settings file	191
8.2.1	WSProperties	192
8.3	WebShare utility programs	193
8.3.1	zipstream	194
8.3.2	unzipstream	196
8.3.3	wcommon.pm	200
8.3.4	Action script environment variables	200
8.3.5	wscopy.pl	201
8.3.6	wsmove.pl	201
8.3.7	wdownload.pl	202
8.3.8	wsdup.pl	202
8.3.9	wsmkdir.pl	202
8.3.10	wsmv.pl	203
8.3.11	wspreview.pl	203

8.3.12	wsforgotpw.pl	204
8.3.13	wsregnewuser.pl	205
8.3.14	warm.pl	205
8.3.15	wsparm.pl	206
8.3.16	wsupload.pl	206
8.3.17	wsuploadmv.pl	206
8.3.18	WebShare File Server service port	207
8.4	WebShare scripts	208
8.4.1	Custom scripts	208
8.4.2	Debugging WebShare scripts	211
8.4.3	Sample action scripts	212
8.4.4	Calling action scripts via JavaScript	215
8.5	Preferences	217
8.5.1	WebShare File Server preference keys	217
8.5.2	Sharepoint preference keys	227
8.5.3	Quickshare preference keys	231
8.5.4	Web Server preference keys HELIOS Admin needs to know	233
9	HELIOS Document Hub	235
10	WebShare security	237
10.1	Security considerations	237
10.1.1	WebShare Web Server	237
10.1.2	WebShare File Server	238

10.1.3	Server setup	238
10.1.4	Firewalls	238
10.1.5	Access from the WebShare Web Server to the WebShare File Server	239
10.1.6	Symbolic links within sharepoints	239
10.1.7	Action scripts	239
10.1.8	Allow all Read or Read/Write access in sharepoints	240
10.1.9	“wsaddshare” and “wslogin” scripts	240
10.1.10	No content security	241
10.1.11	Switching WebShare to port 80 on the WebShare Web Server	241
A	Special characters in file names	243
B	WOSTarter – Web service health check	245
C	Technical notes	247
C.1	WebShare log file structure	247
Index		249

1 About the chapters of this manual

In the following, we give a brief summary of each chapter of this manual. This summary is meant to help you find the information you are looking for.

Chapter 2 “An introduction to HELIOS WebShare” gives background information about the idea of WebShare in general, and the components that make it up.

Software installation on the server

Chapter 3 “Installation” describes the different means of connecting the WebShare Web Server and the WebShare File Server. In addition, the chapter covers the installation of the two-tier server system, including the prerequisites and the final verification of the installation.

WebShare – Administration and use

Chapter 4 “Administration” describes how to administer the WebShare File Server, including server preferences, WebShare Quickshares, users, sharepoints, and accounting (which lists all user actions). The Branding Editor, and WebShare statistics (information on the WebShare Web Server, Java, users, and the license) are discussed as well. The HELIOS Icon Collector, URL Share Access, and the related catalog presentation are also covered in this chapter.

Chapter 5 “HELIOS Admin” briefly shows how to manage WebShare related tasks such as configuring WebShare users and sharepoints with the HELIOS administration program.

Chapter 6 “Using WebShare” provides *step-by-step* user instructions for working with WebShare, including file management, WebShare Quickshares, previews and proofs of images and documents, personal user settings, file format and browser information.

Description of the WebShare server modules

Chapter 7 “WebShare Web Server” gives a listing of installed files. This is followed by a brief guide about WebShare Web Server localization and customization tasks. WebShare Web Server preference keys are described at the end of the chapter.

Chapter 8 “WebShare File Server” is a reference for the WebShare administrator. Utilities and (customizable) scripts and their function are explained as well as configuration files, preferences and accounting files. In addition, their function and effects on the WebShare File Server are described.

Chapter 9 “HELIOS Document Hub”

HELIOS Document Hub allows access to intranet file server volumes to present and use server documents online and offline while a built-in file synchronization ensures that server files are automatically updated on mobile devices.

Chapter 10 “WebShare security” gives background information about server port security issues in general, and also about JavaScript security in the WebShare Web Server. This chapter also addresses how to control access to the WebShare File Server.

Additional information

Appendix A “Special characters in file names” provides information on the use of special characters in file and folder names and their behavior during upload/download processes.

Appendix B “WOSTarter – Web service health check” The HELIOS Service Controller can use this plug-in to start/stop and monitor the WebShare Web Server (“websharewoa”).

Appendix C “Technical notes” describes the structure of the WebShare log files (which can be inspected in the HELIOS Admin `Lists` menu).

2 An introduction to HELIOS WebShare

HELIOS WebShare is a high-performance server, which enables fast and secure real time file access via any web browser. Authorized users, wherever they are, can easily use the file server without exposing it to the internet.

Remote collaboration

Remote collaboration becomes a reality with the fully automated two-way access to the server data. File browsing and management allow authorized users to manage files and folders remotely, similar to the local Windows Explorer or Mac Finder. It offers remote document previews of all major image formats. Remote OPI allows web clients to download OPI low-resolution images from the server and to upload completed documents for later printing with high-resolution images. Remote print job proofing is easy as well. Verification/proof of QuarkXPress, InDesign and PDF documents is also possible (see 2.3 “Integration with other HELIOS products”).

Security

Security is provided by a two-tier server application, comprised of the WebShare Web Server and the WebShare File Server. The WebShare Web Server handles the web user interface on a separate server to ensure that the main WebShare File Server is not available on the internet. The server file system security is enforced according to each user’s credentials. Sharepoint based security allows further restrictions per user, e.g. browse, preview, download, upload and file management. Additional SSL encryption is supported.

Highest performance

Due to zipstream (unzipstream) *on-the-fly* compression (uncompression), HELIOS WebShare provides very fast performance, optimizing use of the internet bandwidth.

Note: HELIOS WebShare runs on top of the foundation provided by HELIOS Base. Please read the HELIOS Base manual for installation instructions and other important details.

2.1 New WebShare features

For new features in the WebShare software see the HELIOS website:

www.helios.de Go to *HELIOS Product Versions – New Features*

For HELIOS Base, the foundation used by all HELIOS products, see the HELIOS Base product web page:

www.helios.de Go to *Products > Base*

2.2 Client file transfer and syncing applications included with WebShare

2.2.1 WebShare Manager

The HELIOS WebShare Manager client tool allows synchronizing files and folders between a WebShare server and remote workstations over the Internet, using any standard web browser.

HELIOS WebShare Manager user manual:

www.helios.de Go to *Support > Media > HELIOS user manuals*

2.2.2 Document Hub

HELIOS Document Hub allows access to intranet file server volumes to present and use server documents online and offline while a built-in file synchronization ensures that server files are automatically updated on mobile devices.

See also 9 “HELIOS Document Hub”.

2.3 Integration with other HELIOS products

WebShare is part of an integrated product suite that enables the enhancement capabilities by adding additional HELIOS products.

Files on the WebShare File Server are stored in the HELIOS resource format as used by EtherShare and PCShare. This preserves special file properties, such as Mac resource forks or Windows file streams. If the WebShare sharepoint is the same as or overlaps an EtherShare or PCShare volume, then custom Mac icons are preserved as well.

If the WebShare File Server is installed on a Windows platform, and the defined sharepoint is in an NTFS partition, the files will be saved to disk in the SFM (*Services for Macintosh*) compatible format.

In case the WebShare File Server is running on OS X – without EtherShare or PCShare being installed – and the defined sharepoint is in an HFS partition, the files will be saved to disk in the native Mac OS format. In that case, file management (duplicate, copy/paste, rename) on OS X utilizes the native OS commands (“cp”, “mv”), which may not preserve the resource fork of Mac files. Custom Mac icons are always preserved on OS X.

HELIOS Base (included with all HELIOS products) includes the “dt tools” for file management. These utilities properly handle Mac resource forks and

Windows file streams during file management, to preserve file type and creator information, file streams, etc. In addition, WebShare sharepoints that are the same as or overlap EtherShare and PCShare volumes will use the “dt tools” to update the desktop database for the HELIOS volume, providing support for Mac custom icons, and full compatibility for WebShare users and EtherShare/PCShare users.

EtherShare and PCShare are fully compatible with WebShare and add advanced file and print servers for Mac and Windows clients, respectively.

HELIOS ImageServer, for server-based OPI, image conversion, workflow automation, and color management, extends the WebShare preview capabilities to InDesign and QuarkXPress documents. WebShare together with ImageServer also enables remote workflow support via hot folders and custom actions.

HELIOS PDF HandShake and ImageServer enable remote PDF-native OPI on WebShare.

HELIOS PrintPreview adds support for remote proofing, annotations, and printing as well as remote separation proofing and color-matched composite previews, which can be remotely viewed or transferred via WebShare.

3 Installation

3.1 Different setups

3.1.1 General overview

WebShare is comprised of two main servers: the WebShare Web Server, and the WebShare File Server. The objective is to enable versatile and high performance remote file access over the internet, while at the same time isolating the file server from the internet. This feature is accomplished by means of the two-tier WebShare server application. The WebShare Web Server acts as an intermediary between the internet and the WebShare File Server:



When remote users log in to WebShare, their only access is to the WebShare Web Server, which is connected to the internet. The WebShare Web Server is very secure, and contains no data, passwords or configuration information. This WebShare Web Server accepts requests and forwards them to the WebShare File Server, via a private protocol. The file server authenticates these requests, and then starts a separate process with each user's access rights, so that remote users can access only the files and directories for which they have file system permissions. The WebShare File Server forwards the requested content to the WebShare Web Server which generates dynamic web pages for the remote users. This enables them to "see" the file server, without being directly connected.

Ideally, the WebShare Web Server application should run on a dedicated server, allowing all other services and ports to be shut down. The WebShare File Server application then runs on the server that contains the actual data to be shared. The following sections detail the various server configurations possible, and the related firewall options. Additional security details are discussed in 10 “WebShare security”.

3.1.2 Software firewall (Internet)

A software firewall can be configured directly on the WebShare Web Server (Fig. 3.1). For example, on an OS X server, software firewall settings can be defined via “System Preferences... > Sharing”. It must only allow incoming HTTP connections, and only on port 2009. Other ports on this server must not be reached from the internet in order to provide a high level of security. Chapter 10.1.11 “Switching WebShare to port 80 on the WebShare Web Server” describes how to change the default HTTP IP address and port.

Furthermore, the WebShare Web Server needs two network interfaces, one for the internet, and one for the intranet. IP-routing must be switched off.

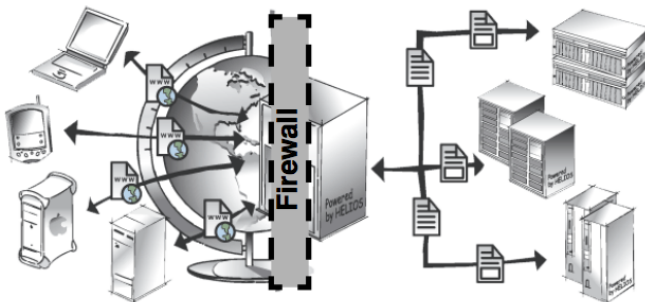


Fig. 3.1: Software firewall towards the Internet

3.1.3 Hardware firewall (Internet)

Another possibility is to install a hardware firewall between the internet and the WebShare Web Server (Fig. 3.2). As described in 3.1.2 “Software firewall (Internet)”, the firewall must only allow incoming HTTP connections on port 2009. Here, one network interface for both the internet and the intranet will do, but two network interfaces offer additional security. IP-routing must be switched off.

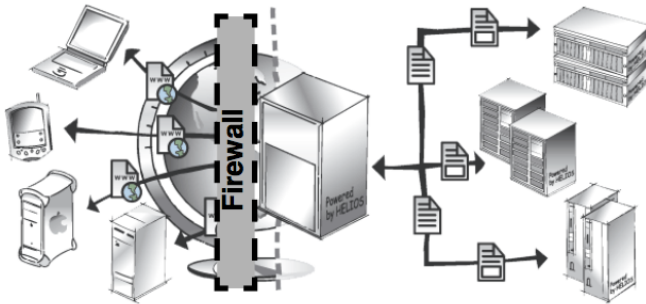


Fig. 3.2: Hardware firewall towards the Internet

3.1.4 Hardware firewall (Intranet)

A hardware firewall can also be positioned between the WebShare Web Server and the intranet. It should only allow incoming connections on ports 2010-2015. In addition, a software firewall should only allow incoming HTTP requests on port 2009 (Fig. 3.3). This setup requires two network interfaces, one for the internet and one for the intranet. IP-routing must be switched off.

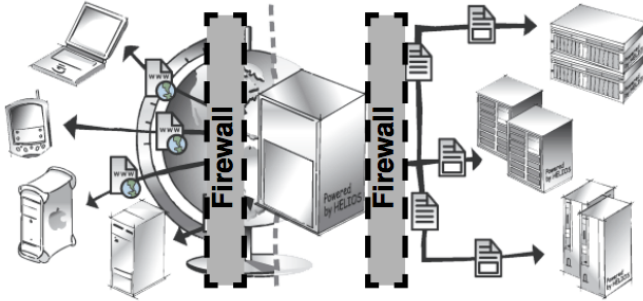


Fig. 3.3: Hardware firewall towards the intranet

3.1.5 Single-server solution

In a single-server solution (Fig. 3.4), the WebShare Web Server and the WebShare File Server are running on the same machine. The hardware firewall must deny incoming HTTP connections other than on port 2009.

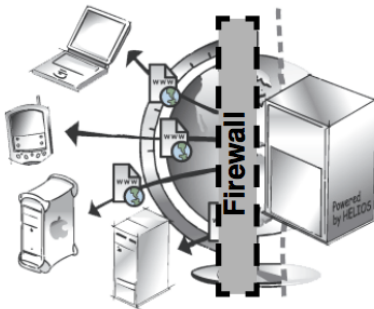


Fig. 3.4: Single-server solution

3.2 WebShare Web Server installation

3.2.1 System requirements

For the installation of the WebShare Web Server the following prerequisites apply:

- Any supported HELIOS server platform. See a current listing of all supported platforms at: www.helios.de/web/EN/support/platforms.html
- The programming language Perl (version 5.8.4 or newer)
- 64-bit Java 6 or newer (see 4.1.2 “Server requirements” in the HELIOS Base manual)
- 32 MB RAM; 2 MB per active client

Note: If a two-tier WebShare server configuration is used, then only HELIOS Base and the WebShare Web Server should be installed on the server that is connected to the Internet. On the WebShare File Server, HELIOS Base and the WebShare File Server get installed. It is only necessary to enter the HELIOS license information on the WebShare File Server.

3.2.2 Software installation

The installation of the HELIOS WebShare Web Server follows the standard HELIOS software installation scheme. It is described in detail in the chapter “Software Installation” in the HELIOS Base manual.

3.2.3 Verifying the installation

There are some steps you should take in order to verify that the installation of the WebShare Web Server was successful:

- On a command line, issue `srvutil status` (see “`srvutil`” in the HELIOS Base manual):

```
$ srvutil status
Service      Status      PID    When      Restarts
srvsrv       Running     28287  Wed 10:08
notifysrv    Running     28289  Wed 10:08
authsrv      Running     28294  Wed 10:08
desksrv      Running     28295  Wed 10:08
heladmsrv    Running     28302  Wed 10:08
afpsrv       Running     28303  Wed 10:08
indexsrv     Running     28290  Wed 10:08
papsrv       Running     28304  Wed 10:08
pcshare      Running     28305  Wed 10:08
lpd          Running     28312  Wed 10:08
websharesrv  Running     28306  Wed 10:08
dhcpsrv      Running     28309  Wed 10:08
opisrv       Running     28313  Wed 10:08
scriptsrv    Running     28307  Wed 10:08
createpdf    Running     28293  Wed 10:08
mdnsproxysrv Running     28297  Wed 10:08
websharewoa Running     28298 Wed 10:08
toolsrv      Running     28308  Wed 10:08
```

The result of the status query shows that “websharewoa” is running. If “websharewoa” is not running, check the system messages for errors.

Note: On OS X systems, the installation can be verified with the “HELIOS Services” application, which is installed in the OS X “Applications” folder.

The following steps may be used to verify that the WebShare Web Server is also available remotely:

- In your browser enter the URL:
http://hostname:2009

If the HELIOS WebShare homepage appears, the installation was successful.

- If it is not, try:

http://<DNS name>:2009

Example:

http://myserver.com:2009

- If this fails, try:

http://<IP-address>:2009

Example:

http://172.16.0.8:2009

If you are successful with using the IP address in the URL but not with “host name” or “DNS name”, the installation of the WebShare Web Server was successful, but you may have a DNS configuration problem.

- Verify with the HELIOS “socket” utility (verbose mode) that the web server can be reached:

```
$ socket -v myserver.com 2009
Trying to connect to myserver.com port 2009 ...
...
Successfully connected to server.
```

- If this returns an unknown host, try the IP address:

```
$ socket -v 172.16.0.8 2009
Trying to connect to 172.16.0.8 port 2009 ...
...
Successfully connected to server.
```

- If this also fails, try (directly on the WebShare Web Server):

```
localhost$ socket -v localhost 2009
Trying to connect to localhost port 2009 ...
...
Successfully connected to server.
```

- Exit “socket” with Ctrl-C.

Note: The host names and IP addresses in the excerpts above are just examples!

Note: By default, the WebShare Web Server allows connecting to all WebShare File Server hosts. The preference **WSAllowedHostNames** (7.6 “Preferences”) restricts the access to named WebShare File Servers only.

3.3 WebShare File Server installation

3.3.1 System requirements

For the installation of the WebShare File Server the following prerequisites apply:

- Any supported HELIOS server platform. See a current listing of all supported platforms at: www.helios.de/web/EN/support/platforms.html
- The programming language Perl (version 5.8.4 or newer)
- 32 MB RAM; 2 MB per active client
- Each server that publishes files via WebShare requires a WebShare File Server license

3.3.2 Software installation and licensing

The installation of the HELIOS WebShare File Server uses the standard HELIOS Installer. It is described in detail in the chapter “Software Installation” in the Base manual.

The license is entered according to the instructions given in the chapter “Entering a new license” in the HELIOS Base manual.

3.3.3 Verifying the installation

There are some steps you should take in order to verify that the installation of the WebShare File Server was successful:

- On a command line, issue `srvutil status` (see “`srvutil`” in the HELIOS Base manual):

```
$ srvutil status
Service      Status      PID   When      Restarts
srvsrv       Running    28287 Wed 10:08
notifysrv    Running    28289 Wed 10:08
authsrv      Running    28294 Wed 10:08
desksrv      Running    28295 Wed 10:08
heladmsrv    Running    28302 Wed 10:08
afpsrv       Running    28303 Wed 10:08
indexsrv     Running    28290 Wed 10:08
papsrv       Running    28304 Wed 10:08
pcshare      Running    28305 Wed 10:08
lpd          Running    28312 Wed 10:08
websharesrv Running 28306 Wed 10:08
dhcpsrv     Running    28309 Wed 10:08
opisrv       Running    28313 Wed 10:08
scriptsrv    Running    28307 Wed 10:08
createpdf    Running    28293 Wed 10:08
monitorsrv   Running    28296 Wed 10:08
mdnsproxysrv Running    28297 Wed 10:08
websharewoa  Running    28298 Wed 10:08
toolsrv      Running    28308 Wed 10:08
```

The result of the status query shows that “`websharesrv`” is running.

Note: On OS X systems, the installation can be verified with the “HELIOS Services” application, which is installed in the OS X “Applications” folder.

The following steps may be used to verify that the WebShare File Server is also available remotely (use the appropriate server host name, or IP address, in place of “helioshost”):

```
$ socket -v helioshost 2010
Trying to connect to helioshost port 2010 ...
...
Successfully connected to server.
```

➤ Exit “socket” with Ctrl-C.

As the example above shows, the WebShare File Server port (2010) is available.

4 Administration

This chapter describes the configuration and administration of the WebShare File Server via the WebShare Administration web page. All WebShare administration can also be performed via HELIOS Admin, with the exception of the Branding Editor, and Java Server Statistics. Refer to 5 “HELIOS Admin” for details.

- Launch a browser and enter the WebShare Web Server address, using port 2009, e.g.: `http://hostname.company.com:2009`

The WebShare Web Server port number can be changed by means of the **WOPort** preference (7.6 “Preferences”).

- Log on to the WebShare File Server according to the instructions in 6.1 “WebShare File Server login”.

In order to have WebShare administrative privileges, a user must log in as “root” (UNIX based servers) or “Administrator” (Windows based servers) or be a member of either the “WSAdm” or the “SysAdm” group. Members of the “SysAdm” group have administrative privileges for HELIOS Admin and WebShare. Members of the “WSAdm” group have administrative privileges for WebShare only.

Important: After the first time installation of a HELIOS product the “root” and “demouser” passwords are empty and should be assigned as soon as possible!

HELIOS Admin is used to set the “root” and “demouser” passwords as described in “Setting passwords” in the HELIOS Base manual. You can then

set additional WebShare host user passwords (see 4.1 “Server Preferences”, below), and assign administrators to the “WSAdm” or “SysAdm” groups. Alternatively, the HELIOS utility program “authutil” can be used to set passwords.

There you will also find a detailed description on how to access and log in to HELIOS Admin.

Note: HELIOS Admin can also be accessed via WebShare, as an administrative user, in the “HELIOS Applications” sharepoint:

- From a Mac client, click on “MacOS”, and select and download the “HELIOS Admin.app”. From a Windows client, click on “Windows”, and select and download the “HELIOS Admin.exe”. For other platforms click on Java, select “HELIOS Admin.jar”, and download.
-

After a successful login to WebShare, the “Home” page appears, allowing quick access to the defined sharepoints (Fig. 4.1).



Fig. 4.1: WebShare “Home” page

-
- Click on the `Administration` button. From within the “Administration” section, select the desired item (Fig. 4.2).

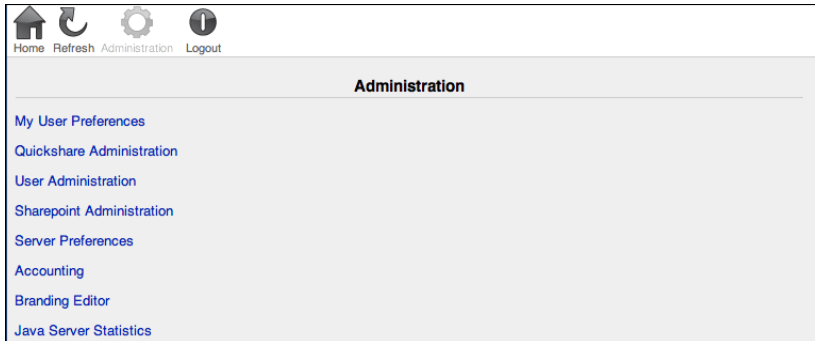


Fig. 4.2: WebShare “Administration” page

4.1 Server Preferences

The “Server Preferences” page (Fig. 4.3) allows specifying default values for the WebShare File Server.

Cache

WebShare keeps image preview files, which have already been displayed, in a cache on the WebShare File Server, so they will open quite quickly the next time they are requested. The `Cache Size in MB` and the path to the `Cache Directory` are specified in the respective fields. If the `Cache Directory` is changed, the new directory must already exist, and have full `rwx` (read-write-execute) privileges for all.

The number of files in the cache is only limited by the assigned cache size. When the cache is full, WebShare starts to delete old files in the cache in order to store newer files. If the `Clear on Save` checkbox is ticked, WebShare deletes all cache files upon clicking the `Save Preferences` button.

Home Refresh Administration Logout

Server Preferences

Cache Size in MB: (A minimum of 300 MB is recommended)

Cache Directory:

Remove All Cache Files: Clear on Save

E-Mail Notification on Admin Login:

E-Mail Notification on User Login:

Enable E-Mail Message for Users:

Enable WebShare for Host Users:

Enable WebShare for Virtual Users:

Directory Listing Date Format:

Default Windows Encoding:

Default Mac OS Encoding:

Max. Gallery Resolution (pixel):

Preview Resolutions (pixel or dpi):

Proof Simulation Profiles:

Custom Preview Types:

Enable Register User Option:

Enable Forgot Password Option:

Enforce RSA Crypted Passwords:

Allow URL Share Access: (reduced security)

Allow Quickshares: (reduced security)

Quickshare Users are Global: (reduced security)

Skip Login With Empty Quickshare Passwords: (reduced security)

Allow ICC Profiles per User:

Default Branding:

Detailed information on the date format is available at: [Java Date Format](#)

Fig. 4.3: "Server Preferences" page

Clearing the cache should be done without any users connected, to avoid login time-outs during the removal. Alternatively, the WebShare File Server can be stopped with the `srvutil stop websharesrv` command and the content of the cache directory subsequently deleted with `rm -r <CACHEDIR>/*`. The WebShare File Server is restarted via `srvutil start websharesrv`.

Note: The default value for `Cache Size in MB` is 30, due to the usually limited disk space in “`HELIOSDIR/var`”. If you change the `Cache Directory` preference to another path, it is recommended to set `Cache Size in MB` to a value of at least 300 (MB).

E-Mail

WebShare acts as an SMTP client and can send e-mail notifications via an SMTP server running on the same host, or via an external SMTP server.

The server settings `SMTPHost` and `SMTPSender` must be set up correctly for e-mail notification to work (see **SMTP** in “`HELIOS Admin > Server Settings`” in the `HELIOS Base` manual).

By use of the `Enable E-Mail Message for Users` option, the administrator can determine whether the `Mail` functionality (see **Edit** > in 6.3 “`Work in a sharepoint`”) is available to WebShare users.

WebShare users

`Enable WebShare for Host Users` and `Enable WebShare for Virtual Users` determine which type of users can connect to WebShare. *Host Users* are those users who are listed in the `HELIOS` password file “`var/conf/passwd`” or who are provided via AD/PDC or LDAP. *Virtual Users* are user names who have been set up as WebShare users only, but are mapped to a host user name (compare 4.3 “`User Administration`”). If `Enable WebShare for Host Users` is not checked, then individual *Host Users* can still be enabled by entering them as *Virtual Users*. If neither checkbox is marked, only “`root`” (or *Virtual Users* mapped to the user “`root`”) can log in.

Important: Host users must have an entry in the `HELIOS` password file “`var/conf/passwd`”. Otherwise they will not be accepted as valid users and hence cannot log on to the WebShare File Server!

Date format

The `Directory Listing Date Format` can be customized, e.g. according to American or European date format preferences. For details go to:

docs.oracle.com/javase/1.5.0/docs/api/java/text/SimpleDateFormat.html

Download encoding

The two pop-up menus `Default Windows Encoding` and `Default Mac OS Encoding` specify the default download encoding for the used client platform. The setting determined here is applied when `OS Default` in the `Download Encoding` pop-up menu (see 6.7 “My User Preferences”) is selected.

Gallery Resolution

The `Max. Gallery Resolution (pixel)` field allows specifying the maximum resolution for image previews which can be selected by use of the slider in the WebShare gallery view. If set to 0 the gallery view is disabled. The corresponding button (`File > Set View > Gallery`) will be disabled or hidden depending on the `Show Disabled Buttons` setting of the used branding. The minimum value allowed (beside 0) is 32.

See 4.7 “Branding Editor” for further details on how the initial and possible gallery resolution values are determined.

Preview options

The `Preview Resolutions (pixel or dpi)` field is used to specify custom resolutions and percentage sizes for remote file previews and proofs. Preview and proof pages include four “zoom icons” for which the resolutions can be defined per branding, in the Branding Editor, by use of the “Preview Resolutions 1-4” preference (see **Toolbar Buttons**). In addition, there is a pop-up menu, which can be used to offer custom resolutions. This makes sense if preview or proof resolutions or sizes are frequently required which differ from the default. The custom pop-up menu dpi, pixel, and percentage values can be specified in the `Preview Resolutions (pixel or dpi)` field, as a comma-separated list. Note that images will not be scaled up from their original resolution (i.e., if the image is 512 pixels, and the user selects 768 pixels, the preview will not exceed 512 pixels). The default values in the pop-up list for previews and proofs are: 36, 72, 96, 144 dpi and 256, 512, 768, 1024 pixel.

Proof profiles

The `Proof Simulation Profiles` field allows specifying profiles, which should be available in the `ICC Proof Simulation` pop-up menu in the WebShare proof window. You can specify any profile that is stored in the “ICC-Profiles” volume.

Note: For this feature the “WebShare Public” sharepoint needs to be published.

If the `Allow ICC Profiles per User` option is enabled, WebShare users are allowed to upload and administer their own monitor and printer ICC profiles on the “My User Preferences” administration page. These profiles will be selectable in the `Monitor ICC Profile` and `Printer ICC Profile` pop-up menus of the WebShare proof window, in addition to any globally defined profiles. To benefit from this feature, HELIOS ImageServer is required.

Custom preview types

In the `Custom Preview Types` field you may enter suffixes for custom file types that are to be previewed in WebShare. For this to work, the files must be processed first (according to the rules given in the “wspreview.pl” script). For example, `doc,xls,ppt` (no blanks!) can be specified for Microsoft Office documents which, if required, are processed by Tool Server with the “OfficeReader” script. “OfficeReader” details can be found in the HELIOS Tool Server manual.

Login options

The setting of the checkboxes `Enable Register User Option` and `Enable Forgot Password Option` determines whether the `Register as a New User` and `Forgot Password?` links become available in the login window.

Note: These options enable the “wsregnewuser.pl” and “wsforgotpw.pl” WebShare utility programs (see 8.3 “WebShare utility programs”). These two sample scripts do not really register a new user, or generate/send a new password, until they have been customized to do so.

With the checkbox `Enforce RSA Crypted Passwords` checked, only encrypted user logins are permitted. For this purpose, JavaScript must be active in the web browser.

URL Share Access

If the checkbox `Allow URL Share Access` is checked, direct access to a specified WebShare sharepoint or to a document preview is possible. See 4.10 “WebShare URL Share Access” for a description on how WebShare link sharing works and what attributes can be set.

Quickshares

Check the checkbox `Allow Quickshares` to allow Quickshares on the WebShare server. While creating a Quickshare, a user can select the desired remote user from the `User` pop-up menu in the “Quickshare” section of the sharepoint file browser. If the `Quickshare Users Are Global` checkbox is checked, *all* Quickshare users are available in this pop-up menu. If not checked, only those Quickshare users who were created by the logged-in user are available. `Skip Login With Empty Quickshare Passwords` can be checked if the remote user should be allowed to open the Quickshare links by just clicking on them, without a prior login on the WebShare server (then the password must remain empty).

Branding

The pop-up menu `Default Branding` allows pre-selecting a global branding for all users on the WebShare File Server. This setting can be overridden for individual users by the setting of the `Branding` pop-up menu on the “User Administration” page (see 4.3 “User Administration”).

- Click on the `Save Preferences` button to save modifications. Otherwise the changes will not be saved and will be lost.

4.2 Quickshare Administration

The “Quickshare Administration” page allows users to activate/deactivate existing Quickshares, delete them, or edit their corresponding comments, expiry dates, and permissions (Preview, Download, Upload). In addition, single Quickshares can be re-assigned to a different user. Non-administrators will see only the Quickshares that they have created, as discussed in 6.6.2 “Manage your own Quickshares”. WebShare administrators will have an additional option, `Show All Quickshares`, which lists all existing Quickshares.

However, the fields `Quickshare ID`, `URL`, `Sharepoint`, `Path`, and `Files` are provided for informational purposes and cannot be edited.

Note: *The E-Mail on Access function will be available in a future version of WebShare:*

When the user who was provided with the Quickshare link accesses the WebShare server, the creator of the Quickshare can optionally be notified.

Delete Quickshares

➤ Select a Quickshare from the table and click on the `Delete Quickshare` button. Then confirm the deletion.

Important: Do not click on `Save Changes` at this point because the data entry fields still contain the user information, and hence the Quickshare will be re-created!

The “Select” column allows selecting/deselecting all displayed Quickshares at a time.

Home Refresh Administration Logout

Quickshare Administration

My Quickshares | Show All Quickshares

Active:

Quickshare ID:

URL: [Open](#)

Quickshare User: [+](#)

Creator:

Sharepoint:

Path:

Files:

Allow: Preview - Download - Upload

Expires: (e.g.: 18 Mar 2014 15:24)

Comment:

E-Mail on Access:

[Save Changes](#) [Delete Quickshare](#) [Send mail to Bart](#)

[Select All](#) | [Deselect All](#)

Select	QS ID	QS User	Active	Expires	Sharepoint	Path	Files	Comment
<input type="checkbox"/>	1	Bart	<input checked="" type="checkbox"/>	15 Jan 2020 16:16	Sample Images	template-images%0	Cafeteria.tif	
<input type="checkbox"/>	2	heinz	<input type="checkbox"/>	18 Aug 2020 19:35	Sample Images	template-images%0	IL14_0056.pdf	Check color profile!

Fig. 4.4: WebShare “Quickshare Administration” page

4.3 User Administration

The “User Administration” page (Fig. 4.5) allows WebShare administrators to specify settings for users. Here WebShare virtual users can be created and deleted, and WebShare-only passwords specified for host users. Users can be assigned preset values for Download Encoding, Zip Streaming Format, and Branding. Some of these settings can be changed by the users themselves on their “My User Preferences” administration page (6.7 “My User Preferences”).

In addition, there is the `Privileged Transfer` option which reserves a higher transfer bandwidth for the corresponding user. For all other users, file transfers will then (and only then!) be restricted to a limited speed (5 to 80 kB/s, depending on the currently used Internet connection).

User Administration

User Name:

Password: (Crypted RSA 1024 bit)

Cannot change Password:

Run as Host User:

E-Mail Address:

Comment:

Expires: (e.g.: 18 Mar 2014 14:53)

Download Encoding:

Zip Streaming Format:

Privileged Transfer:

URL Document Preview only:

Quickshare User:

Branding:

User Name	Run as Host User	QS User	Branding	Expires	Comment
Bart	demouser	<input checked="" type="checkbox"/>	Server Default		
Bender	root	<input type="checkbox"/>	Futurama		

Fig. 4.5: WebShare “User Administration” page

The URL Share Access feature allows sharing documents without letting the user navigate out of the document preview. If the `URL Document Preview only` checkbox is activated the user (except a user with administrative WebShare privileges!) can only access WebShare by a URL Share Access link that points directly to a document. The user will not be able to leave the document preview then. See 4.10 “WebShare URL Share Access” for further information.

If the `Quickshare User` checkbox is checked the user can only access the defined Quickshare(s). If no Quickshare is defined, the user cannot login at all. The Quickshare status of a user can be seen in the “QS User” column of the user table (see Fig. 4.5).

Normally, new Quickshare users are created by authorized users when they create a new Quickshare and select the `Create new user` option (see 6.6.1 “Create Quickshares”). This has the advantage that a WebShare administrator is not needed to create each Quickshare user or designate files to share. In addition, the file permissions (and WebShare branding) of the user creating the Quickshare are enforced for the new Quickshare user. The sharepoint settings `Allowed Users/Groups` and `Allow Quickshares` control who can create Quickshares, and for which sharepoints (see 4.5 “Sharepoint Administration”).

Important: With the `Quickshare User` checkbox checked, Quickshare users can only log in on the WebShare server if at least one Quickshare has been assigned to them. In addition, they only see their Quickshares!

Notes for WebShare on Windows

Windows local users as well as AD/PDC user names, groups and passwords are automatically supported by WebShare. Host user password changes must be done with the respective tools within Windows. Changing the host user password is not supported within WebShare.

Virtual users are created and managed within WebShare. A virtual name, e.g. *Customer A* does not exist as a host user. However, each virtual user must be assigned to a valid host user account, e.g. “webtransfer”, using the WebShare `Run as Host User` setting. In this case, the host user “webtransfer” must exist with a valid password on the host and the identical user and password must be created using the HELIOS “authutil” command.

Example:

The Windows host user name and password are:

```
User: webtransfer
Password: secret
```

An identical host user and password must be created via the HELIOS “authutil” tool in the HELIOS password file:

```
# authutil passwd -n webtransfer -p secret
```

WebShare virtual users can change their WebShare password within WebShare in Administration > My User Preferences.

Note: Only the *virtual user* password is changed. The password for the corresponding host user remains unchanged.

Like the HELIOS Admin administrative groups “SysAdm”, “PrnAdm”, “QueueAdm”, the administrative group “WSAdm” must be created via Windows to allow control of administrative rights within HELIOS Admin.

Create users

To create a WebShare user take the following steps:

- In the `User Name` field enter an arbitrary name which need not exist on the host, and can have up to 64 characters. Of course, you may also enter the name of an existing HELIOS user on that host. Then assign a password to the user in the `Password` field.

Note: Although a WebShare *virtual user* can have an empty password assigned by the administrator, they cannot delete their password by themselves. A *host user* need not have a WebShare password, but it is highly recommended for security reasons. See **Change WebShare Password** in 6.7 “My User Preferences”.

With the `Cannot change Password` checkbox ticked, users are prevented from modifying their password.

If the user specified in the `User Name` field is not a host user, then that new user will be a virtual user. That virtual user name must be mapped to a HELIOS host user name in the `Run as Host User` field (note that the specified host user *must* already exist on the host).

Note: It is important to note that “Run as Host User” means that the virtual user will have the file access permissions of that host user. In addition, the virtual user will see in the “User” pop-up list (when creating or modifying a Quickshare) any Quickshare users created by that host user, or by other virtual users mapped to that host user. Likewise, host users that have virtual users mapped to them, will be able to see any Quickshare users created by those virtual users.

If an `E-Mail Address` is specified, it appears in the individual user settings (see 6.7 “My User Preferences”). This e-mail address is used as the “From:” e-mail address if that user uses the mail feature. If this is left blank, then that user cannot send e-mail using WebShare. The next two fields are optional and need not be filled out: `Comment` serves as a means to provide additional information on the WebShare user, e.g. to which company or department they belong (see Fig. 4.5). An expiry date, after which the user cannot log in anymore, may be specified in the `Expires` field. The syntax must match that from the example next to the field.

`Download Encoding` specifies the default download encoding for the user client platform. The setting determined here is applied as the default in the `Download Encoding` pop-up menu (see 6.7 “My User Preferences”). With the `Zip Streaming Format` checkbox ticked, the file download uses Zip streaming, which allows file compression *on-the-fly*, without creating any temporary files.

- After creating a WebShare user or configuring existing users, click on the `Save Changes` button before proceeding to other tasks. Otherwise the entries will not be saved. To clear all data entry fields and set the `Download Encoding` and `Zip Streaming Format` back to the default values, click on the `Clear Form` button.

Delete users

- Select a user from the table, click on `Delete User` and confirm the deletion.
-

Important: Do not click on `Save Changes` at this point because the data entry fields still contain the user information, and hence the user will be re-created!

For a correct table display you may need to update the window by clicking on the `Refresh` button in the WebShare toolbar. The table listing the WebShare users can be sorted by clicking on the desired column header.

Note: Deleting users removes only virtual users, and host user WebShare passwords.

Disconnect users

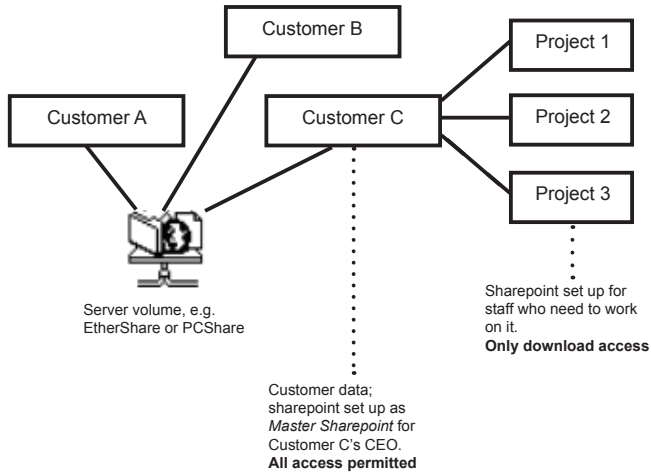
In the event that a system administrator needs to drop a user connection, there are three primary methods:

- Using WebShare, go to “Administration > Java Server Statistics”, and under “WebShare User Statistics”, click `Session Details. Show`. Terminate the desired session.
- Using HELIOS Admin (`Lists > Active Users`), show the connections and delete one of them.
- Or use the `swho -c` command (see HELIOS Base manual) to list active users and the corresponding process ID (*pid*). Then `kill -TERM pid` can be used to terminate that process.

4.4 Organize sharepoints

WebShare sharepoints can be organized to suit the required demands, for example, of a production site. The diagram below shows an example where a HELIOS EtherShare or PCShare volume is published via WebShare. At *Customer C's* site only the CEO is allowed to have full read and write access to the volume. However, the sharepoint is configured to the effect that the staff at *Customer C's* site is only allowed download access. Each user is only able to see their own projects. It is possible to share the same projects for different users with individual permissions.

A WebShare sharepoint can have different task and action rights for different users or groups:



4.5 Sharepoint Administration

Home Refresh Administration Logout

Sharepoint Administration

Publish:

Sharepoint Name:

Sharepoint Path:

E-Mail on Access:

Comment:

Allow Preview: Allow Copy: Always Allow Reading:

Allow Download: Allow Delete: Always Allow Read/Write:

Allow Upload: Allow Rename:

Download Layouts Only: Allow Annotations:

Allow Quickshares:

Allowed Users

Allowed Groups

▼ Document Hub Sync List

VIDEO
catalogo_caberg_2011.pdf

[Add Files & Folders](#)

Show Allowed Users and Groups

Publish	Sharepoint Name	Path	Comment	Sync List
<input checked="" type="checkbox"/>	Demo	/Volumes/Daten/demovol/		Show Disk Usage
<input checked="" type="checkbox"/>	HELIOS Applications	public/		Show Disk Usage
<input checked="" type="checkbox"/>	Sample Images	/Volumes/Data/sample-images%0/		
<input checked="" type="checkbox"/>	WebShare Public	public/WebShare/		

Fig. 4.6: WebShare “Sharepoint Administration” page

With the “Sharepoint Administration” page (Fig. 4.6) WebShare sharepoints can be created, configured or deleted.

The sharepoint “WebShare Public” is created under the path “HELIOSDIR/public/WebShare” during the installation. By default, it has no write access. In addition, the volume “HELIOS Applications” is created for the user “root”. It has no write access either.

Create sharepoints

- In the `Sharepoint Name` field enter the name you want to assign to the sharepoint, and then specify the `Sharepoint Path`. (Note that the specified path *must* already exist with adequate access rights on the host.)
- In the (optional) `E-Mail on Access` field enter an e-mail address for notification mails after a user has downloaded, uploaded, deleted or just previewed a file, or added an annotation. If an annotation has been added to a preview or proof document, the notification e-mail contains a URL share access link which leads directly to the annotation table (the e-mail is sent as soon as the user has logged off or changed the sharepoint). Make sure that the complete recipient e-mail address is specified, e.g.

webshare@mycompany.com

The optional `Comment` field allows entering additional information about the sharepoint. The comments are displayed on the “Home” page (see Fig. 4.1).

With the `Publish` checkbox at the top of the window you can specify if the sharepoint is available at all.

The following options determine whether the buttons in the sharepoint toolbar are enabled (or visible, depending on the “Show Disabled Buttons” setting; see Fig. 4.16):

`Allow Preview`

Allows previews of documents and image files (see 6.4 “Image and document

previews” for complete details). Please note that this checkbox must also be activated to allow viewing documents in proof mode.

Allow Download

Allows the download of files and folders from the respective sharepoint.

Allow Upload

Allows the upload of files and folders to this sharepoint. If desired, Zip archives are automatically extracted.

Download Layouts Only

Specifies that only files inside layout folders in the sharepoint can be downloaded. Layout files are low-resolution proxy files created by ImageServer, for use in OPI aware page layout applications.

Note: The `Download Layouts Only` function requires that `Allow Download` is also active. Otherwise no download action will be possible at all.

Allow Copy

Allows copying, moving, duplicating and pasting files and folders. Also allows creating directories by use of the `Create Dir` option in the `File >` pop-up menu.

Allow Delete

Allows the deletion of files and folders.

Allow Rename

Allows renaming a file or folder.

Note: Changing permissions is only allowed if also `Allow Rename` is allowed.

Allow Annotations

Allows attaching annotations to a document in this sharepoint.

Allow Quickshares

Allows creating WebShare Quickshares on this sharepoint.

Always Allow Reading

Allows file and folder read access for all WebShare users, regardless of their host file and folder permissions. This option only affects the downloading or previewing of files.

Always Allow Read/Write

Allows file and folder read/write access for all WebShare users, regardless of their host file and folder permissions. This option only affects the uploading, downloading or previewing of files, *NOT* other file management options (e.g. copy/move/paste).

Note: The **Always Allow Reading** and **Always Allow Read/Write** options will only be available if enabled by a preference key setting. See **AllowAllRead-Write** in 8.5 “Preferences”.

The **Allowed Users** and **Allowed Groups** fields serve as a means of access control for the sharepoint:

If there are no entries in either of the fields, *all* WebShare users can access the sharepoint. Entries in the **Allowed Users** field allow only those particular users to access the sharepoint. Likewise, entries in **Allowed Groups** allow *only* members of those groups to access the sharepoint. Users who are not allowed access to a sharepoint will not even see it, it will be hidden from them.

Note: Valid names in the **Allowed Users** field may be WebShare user names or host user names. The **Allowed Groups** field accepts valid host group names. Each entry must be in a separate line.

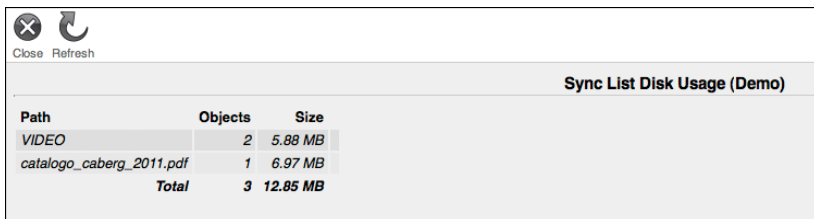
Sync list

The `Document Hub Sync List` link (see Fig. 4.6) allows you to define files or folders in a sharepoint that should be synchronized with the mobile device via the HELIOS Document Hub solution:

- Click on the link and specify the desired files and folders in the text field, or select them by clicking on the `Add Files & Folders` link that opens a new window in which you can select the desired files and folders.

After clicking on `Add Selection` and `Append to Sync List` the selected objects are added to the text field and will be synchronized with the mobile device on request.

A click on the `Show Disk Usage` link in the “Sync List” column opens a new window which gives information on the sync list disk usage (see Fig. 4.7).



Sync List Disk Usage (Demo)		
Path	Objects	Size
VIDEO	2	5.88 MB
catalogo_caberg_2011.pdf	1	6.97 MB
Total	3	12.85 MB

Fig. 4.7: Sync list disk usage

- After creating a WebShare sharepoint or configuring existing sharepoints, click on the `Save Changes` button before proceeding to other tasks. Otherwise the entries would not be saved and get lost. To clear the data entry fields click on the `Clear Form` button.

To set up different access rights for the same directory on the WebShare File Server you can create multiple sharepoints, with the same path but each with a unique name and different access rights (`Allowed Users`, `Allowed Groups`).

Likewise, it is possible to set up different file management and previewing options for the same directory on the WebShare File Server by creating two sharepoints, with the same path but different allowances.

After creating a sharepoint you may wish to view the file permissions corresponding to the sharepoint content:

- Click on the `Home` button, and then on the desired sharepoint. Use `File > Set View > Extended` to view the “Permissions”. If you need to change the permissions, refer to **File >** in 6.3 “Work in a sharepoint” for details.

These permissions will be inherited by any files uploaded via WebShare, and hence determine which users will be able to view files, and change file permissions. Likewise, you may wish to change the file permissions for any existing files in the sharepoint, to enable the desired access for users.

Delete sharepoints

- Select a sharepoint from the table and click on the `Delete Sharepoint` button. Then confirm the deletion.

Important: Do not click on `Save Changes` at this point because the data entry fields still contain the sharepoint information, and hence the sharepoint will be re-created!

For a correct table display you may need to update the window by clicking on the `Refresh` button in the toolbar. The table listing the sharepoints can be sorted by clicking on the respective column header.

Define as HELIOS volume

In general, every WebShare sharepoint should also be the same as or a subset of a HELIOS volume, to ensure that files with Mac resource forks or Windows file streams get handled properly, and in order to enable Spotlight searches within that sharepoint. Use HELIOS Admin (“Volumes” in the Base manual) to define a volume (it need not be published) on each unique top level share.

Lower level shares must NOT have their own (nested) volume definition. In the case that neither EtherShare nor PCShare is installed, HELIOS Admin can still be used to define volumes.

4.6 Accounting

The “Accounting” page (Fig. 4.8) lists all user actions on the WebShare File Server. The default view displays `User`, `Action`, `Time`, `Sharepoint`, `Path` and `Entry` per action.

The exact WebShare status codes are detailed in C.1 “WebShare log file structure”.

Accounting

Log File Date: 08 Oct 2019

Platform Statistics: iMobile: 12.02% Linux/Unix: 0.12% iPhone: 3.62% Windows: 0.49% Mac Intel: 64.62% Mac: 19.13%

Session Count: 35

Today

■ Login Error
■ Generic Error

No	User	Action	Time	Sharepoint	Path	Entry
1	root(14)	login	08:58			
2	root(14)	addUser	09:47	root		
3	root(14)	logout	09:47			
4	root(15)	login	09:47			
5	root(15)	logout	10:48			
6	root(16)	download (Details)	11:42	WebTest	/	Cafeteria.tif
7	root(16)	logout	12:07			
8	root(17)	login	13:12			
9	root(17)	logout	13:59			
10	root(19)	login	14:01			
11	root(19)	logout	14:02			
12	hendrik(1)	login	12:10			
13	hendrik(1)	logout	12:13			
14	hendrik(2)	login	12:13			
15	hendrik(2)	logout	12:14			
16	root(3)	login	12:14			
17	michael(4)	login	12:18			
18	root(3)	logout	12:20			
19	root(5)	login	12:20			
20	root(5)	logout	12:21			
21	hendrik(6)	login	12:21			
22	hendrik(6)	logout	12:21			
23	root(7)	login	12:21			
24	root(7)	logout	13:23			
25	root(8)	login	13:39			
26	root(8)	logout	13:39			

Fig. 4.8: WebShare “Accounting” page

By means of the pop-up menu you can choose which accounting file is displayed on the “Accounting” page. The content is taken from the files “webshare.acct” (*today*) to “webshare.acct.6” (*seven days ago*), which are stored in “HELIOSDIR/var/adm”.

By use of the toolbar item `Set View` you can change the design of the list: `Default` (as seen in Fig. 4.8), `Extended` (includes “Path”, “user agent” (browser), “OS” and “platform” information, and states the date in the “Time” column), and `Small`. A click on column headers changes the sort order. An entry can appear with a yellow or red background. *Red* is used to highlight security warnings (e.g. login errors). *Yellow* is used for informational warnings (e.g. download errors).

Detailed accounting information (Fig. 4.9) for uploaded and downloaded archives is available when clicking on the `(Details)` link.

Accounting Details					
Accounting Information					
Time: 05 Jul 2019 16:50	Sharepoint Path: WebTest:/				
User: root(9)	Action: upload (1 File, 6.4 KB)				
Client: 172.16.0.2	Archive Name: RagTime 6.6.5.rtf.zip				
Success: Yes					
Archive Details (Logfile root-1183646991-3-2812)					
File Name	Modified	File Size	Compressed Size	Deflated	
<i>wsGB-e.pdf</i>	01 Nov 2019 07:52	2.49 MB	1.7 MB	31.74%	
<i>baseGB-e.pdf</i>	12 Oct 2019 11:06	3.06 MB	1.85 MB	39.60%	
<i>esGB-e.pdf</i>	13 Oct 2019 12:14	1.42 MB	943.6 KB	35.00%	
<i>isGB-e.pdf</i>	30 Sep 2019 17:19	2.26 MB	1.53 MB	32.25%	
<i>pdfhGB-e.pdf</i>	12 Oct 2019 10:36	4.26 MB	3.48 MB	18.29%	
<i>ppvGB-e.pdf</i>	30 Sep 2019 17:23	597.3 KB	376.2 KB	37.01%	
<i>psGB-e.pdf</i>	30 Sep 2019 17:16	910 KB	452.3 KB	50.29%	

Fig. 4.9: WebShare “Accounting Details” page

Note: Downloads from a WebShare sharepoint are always archives. Therefore every download action features the `(Details)` link.

4.7 Branding Editor

WebShare features a so-called “Branding Editor”, which allows adjusting the GUI on a per client basis (Fig. 4.10). Clients can thus bring their corporate design into WebShare, which has the following advantages:

- Easy GUI customizing without programming
- Use of corporate designs
- Enhanced customer retention
- Hosting content for different clients on the same server
- Icon families of different skin, color, and size included

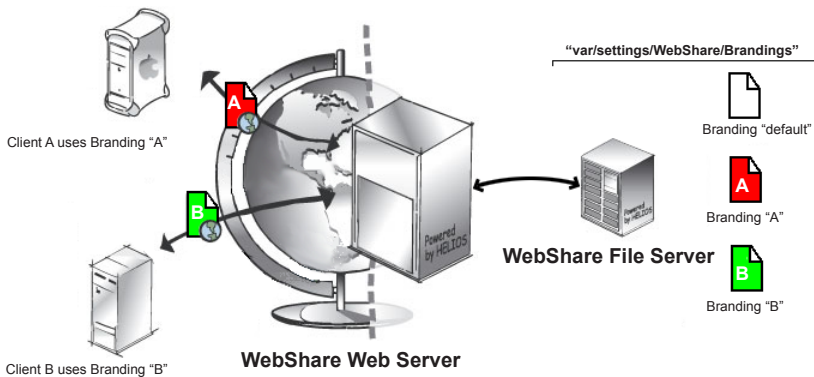


Fig. 4.10: WebShare brandings

4.7.1 Create and configure brandings

All branding components are stored on the WebShare File Server in the “Settings” volume in “WebShare/Brandings/<branding name>”. You may copy images to this folder, they will then be available in the Branding Editor pop-up menus.

The WebShare “default” branding can be used as a template for custom brandings:

- Log on to the WebShare File Server.
- Click on the `Administration` button and select the `Branding Editor` link.

Note: Whenever the Branding Editor is invoked for the first time after the start of the WebShare Web Server, the brandings are synchronized between the WebShare File Server and the WebShare Web Server. Therefore it can take some seconds until the “Branding Editor” is displayed.

- In the “default” branding line click on the `Duplicate` link, enter a name for the new branding and click on the `Save Branding` button.

Note: Use only the characters A-Z, a-z, numbers 0-9, minus (“-”), and underscore (“_”) for the branding names.

The duplicated branding (in the example named “HELIOS”) is now listed in the “Branding Name” column. See Fig. 4.11.

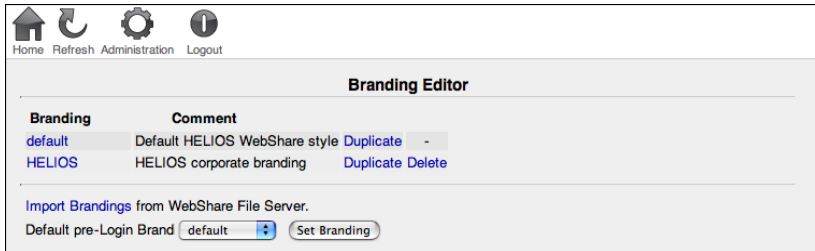


Fig. 4.11: “Branding Editor” page

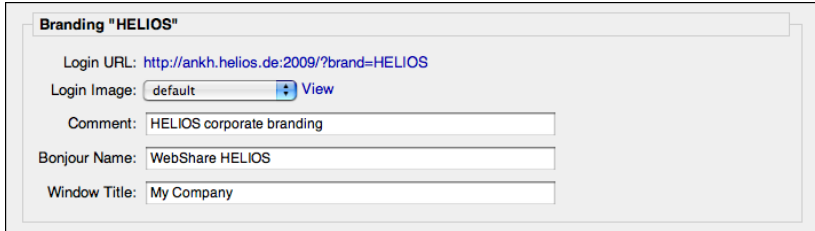
Due to the duplication, the new branding initially comes with the same settings and configuration as the “default” branding. The branding can now be customized:

- Click on the branding name link (in this case “HELIOS”) to open the editor.

Branding

This section (Fig. 4.12) shows the login URL, which includes the branding name and the default for the window title (if this field is left empty, the value “HELIOS WebShare” is assumed). If a window title is specified in the Branding Editor, the `Powered by HELIOS WebShare` link is not displayed anymore for this branding on the WebShare start page, and when logging off from WebShare, the string “Thank you for using HELIOS WebShare.” is replaced with your window title value (“Thank you for using <your_value>”). In addition, this section offers a pop-up menu to choose a login image, a comment field, and a field to enter a name under which the branding appears in the “Bonjour” network environment, e.g. in Apple’s Safari browser (see arrow in Fig. 4.13).

- Click `view` to open a preview of the chosen login image in a new window.



Branding "HELIOS"

Login URL: <http://ankh.helios.de:2009/?brand=HELIOS>

Login Image: default [View](#)

Comment: HELIOS corporate branding

Bonjour Name: WebShare HELIOS

Window Title: My Company

Fig. 4.12: "Branding" section

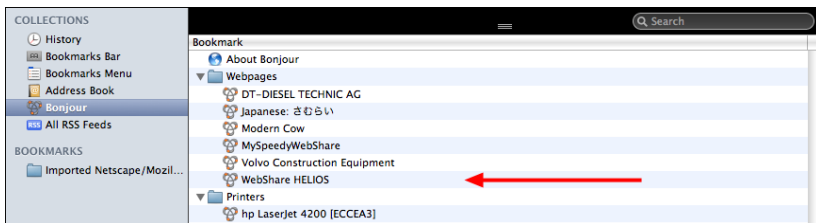


Fig. 4.13: Bonjour listing in Safari

The login URL (Fig. 4.12) can be provided to users who should see and use this branding. Those users must also be assigned this same branding via the "User Administration" page (4.3 "User Administration"). Using the branding login URL ensures that the user is shown the branding login image (Fig. 4.12) and login page corresponding to that branding, even though the user has not yet logged in. Once the user logs in, the branding that has been assigned for that user via the "User Administration" page will be used.

If users navigate to the WebShare server without using their branding login URL, they will see the login image and login page which has been set via the `Default pre-Login Branding` pop-up menu (Fig. 4.11). If a user was not assigned a branding, once they log in, they will see the default branding defined on the "Server Preferences" page (4.1 "Server Preferences").

Body

Each page in WebShare is generated as an HTML page. This section allows defining colors, background images, font family, sizes, etc. (Fig. 4.14).

The screenshot shows the 'Body' configuration panel with the following fields and values:

- Text Color: #000000
- Background Color: #efefef
- Separation Line Color: #d0d0d0
- Background Image: none
- Background Image Attachment: scroll
- Background Image Repeat: no-repeat
- Font Size: 10 pt
- Font Family: sans-serif
- Preferred Fonts: Helvetica, Arial
- Link Color: #0000b0
- Link Rollover Color: #b00000
- Head Banner Image: none
- Head Banner Alignment: left
- Foot Banner Image: none
- Foot Banner Alignment: left
- Vertical Toolbar Padding: 0 pt
- Image Preview Background Color: #f8f8f8

A color picker dialog is open over the 'Link Rollover Color' field, showing a grid of 216 web-safe colors, 142 named colors, and a color slider.

Fig. 4.14: “Body” section

Next to each color definition field is a preview of the specified color. If you click on this square a color picker opens allowing you to pick a color. The color picker supports three modes (Fig. 4.14):

- 216 web-safe RGB colors
- 142 defined named colors
- RGB color slider
(Click on preview field to apply the selected color)

All color definitions can be entered in the corresponding fields either with their name according to the HTML standard (“red”, “black”, “green”, etc.), in their hexadecimal value (e.g. #000000 for “black”) or as RGB values. You may enter “transparent” into a color definition field or leave the field empty, to assign transparency. The following table lists possible color definitions according to the CSS2 specification:

Value	Example	Description
HTML color name	maroon	–
#rrggbb	#CC0066	Hex 6 digits
#rgb	#C06	Hex 3 digits
rgb(rrr, ggg, bbb)	rgb(204, 0, 102)	Decimal RGB
rgb(rrr%, ggg%, bbb%)	rgb(80%, 0%, 40%)	Decimal RGB in percentage notation
<i>Enter “transparent” or leave empty</i>	transparent	Transparency

Note: RGB values, e.g. of corporate spot colors, can be determined by using color meters (e.g. Photoshop Eyedropper tool) and reading out the values from the color picker. These can then be entered in the color value text field, or “reproduced” with the color sliders of the color picker.

The “Vertical Toolbar Padding” setting only addresses Internet Explorer 6 users. It allows specifying the padding between the button strings and the toolbar background. Of course, this setting only applies if the toolbar alignment is set to `vertical`.

Tables

In this section the background colors for even and odd table rows can be defined (Fig. 4.15). It is advisable to specify background colors that contrast with each other, in order to enhance the readability of rows in larger table listings.

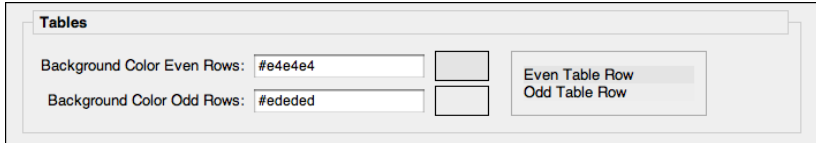


Fig. 4.15: “Tables” section

Toolbar

This section allows specifying the appearance of the WebShare toolbar (Fig. 4.16). The toolbar can be aligned horizontally or vertically, and a background color and a background image can be assigned to it:

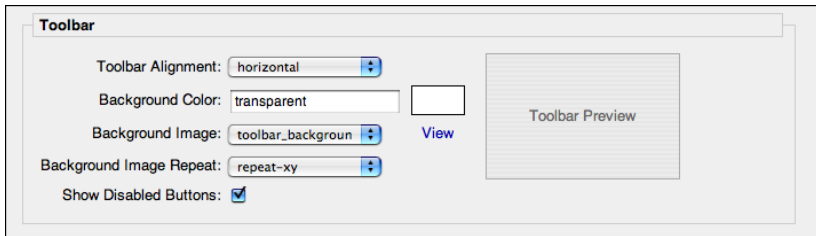


Fig. 4.16: “Toolbar” section

- Select from the pop-up menu whether the toolbar background image should be repeated vertically (`repeat-y`), horizontally (`repeat-x`) or in both directions (`repeat-xy`). If `no-repeat` is selected, the background image is *not* repeated at all, i.e. it only appears once.

If the `Show Disabled Buttons` checkbox is active disabled buttons and menu items appear grayed-out, else they are hidden.

Toolbar Buttons

This section allows specifying the appearance of the WebShare toolbar buttons (Fig. 4.17):

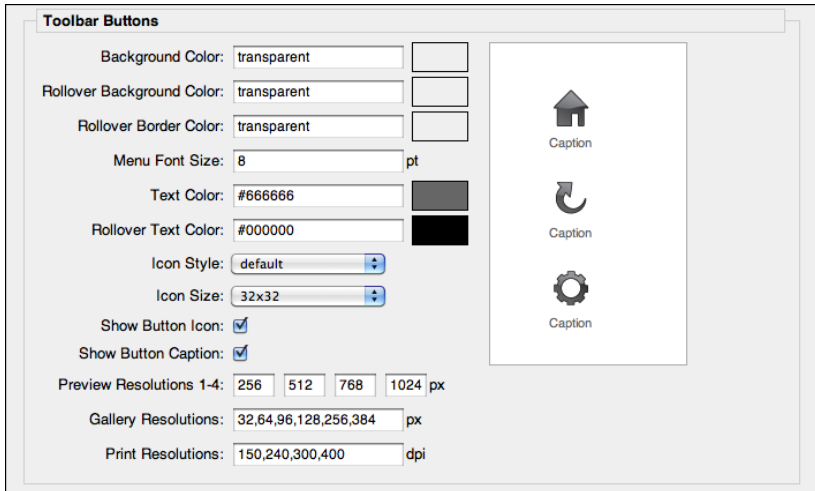


Fig. 4.17: “Toolbar Buttons” section

Some configurable items in this section were already described above in other sections.

Icon styles and sizes can be selected from the corresponding pop-up menu.

If the `Show Button Icon` checkbox is not active, icons are hidden and only the button caption is visible.

If the `Show Button Caption` checkbox is not active, captions are hidden and only the button is visible.

The values specified in `Preview Resolutions 1-4` are used in the 4 zoom buttons (numbered 1-4) for file previews and proofs. Default values are: “256,512,768,1024”.

The `Gallery Resolutions` preference is a comma-separated list of pixel resolutions for the slider control in the gallery view. If only one value is defined the slider control will not be displayed in the gallery view. If the value 0 is defined the gallery view will be disabled for this branding.

This property is limited by the server preference `Max. Gallery Resolution` (4.1 “Server Preferences”) which defines the maximum allowed resolution for gallery previews. Values larger than `Max. Gallery Resolution` can be defined, but the slider control will only allow resolutions up to the value defined in `Max. Gallery Resolution`. The initial resolution of the gallery view is the nearest defined value smaller than or equal to 128 pixels or to the value defined in `Max. Gallery Resolution` if it is less than 128 pixels. Default values are: “32,64,96,128,256,384”.

The `Print Resolutions` preference allows you to specify print resolution values, which are available in the `Resolution` pop-up menu of the print and proof print settings menu. The first four values specified for this preference appear as `Draft`, `Good`, `Excellent`, and `Super Fine`. All other values, starting with the fifth specified value, are displayed as `Custom 1`, `Custom 2`, etc. (see also 6.4.7 “Preview/proof print settings”).

Welcome Message

You may define a welcome message (Fig. 4.18) for the WebShare “Login” page (Fig. 4.19). HTML tags are allowed to format the text.

You may also include an image (in the example below the HELIOS logo) in the login window. See `#loginImage` in 4.7.8 “Customize brandings via CSS” for details.

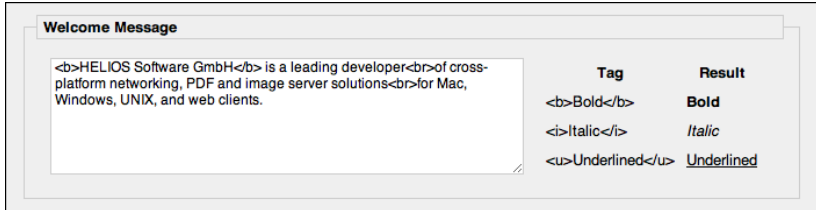


Fig. 4.18: “Welcome Message” section

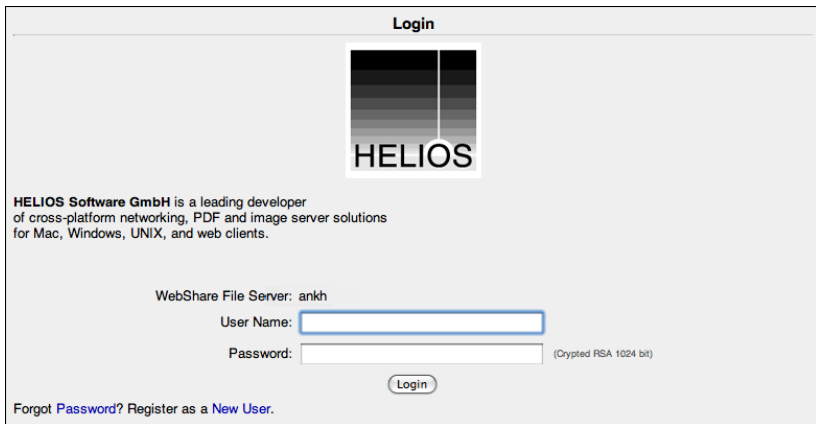


Fig. 4.19: “Welcome Message” at login

4.7.2 Import brandings

You may also import WebShare brandings, which have previously been created, e.g. with the Branding Editor on another WebShare server.

➤ Copy the branding to “var/settings/WebShare/Brandings”.

- Click on the “`Import Brandings from WebShare File Server.`” link on top of the Branding Editor.

Note: While importing brandings, the WebShare Web Server synchronizes with the WebShare File Server. Therefore it can take some seconds until the imported branding(s) appear(s) in the list.

All brandings in “`var/settings/WebShare/Brandings`” will be imported into the Branding Editor and are listed in the “Branding” column (Fig. 4.20; compare with Fig. 4.11).

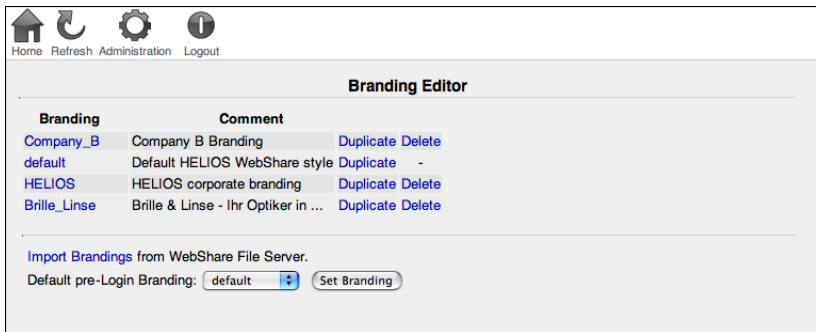


Fig. 4.20: Imported brandings

4.7.3 Brandings and the “style” file

Each branding folder contains the file “style” which stores all branding settings. However, to back up a branding you should save the whole branding folder.

4.7.4 Add custom file icons

For a description of how to add custom file icons to WebShare see **Custom icons** in 4.9 “HELIOS Icon Collector”.

4.7.5 Add custom banner images

WebShare allows having custom head and foot banners per branding (see Fig. 4.14).

- Copy the image that you want to use as banner image into the brandings folder (“WebShare > Brandings > <branding name>”).
- On the “Branding Editor” page click the “Import Brandings from WebShare File Server.” link.
- In the “Body” section select from the pop-up menu `Head Banner Image` (or `Foot Banner Image`) the desired image file and confirm with the `Save` button.

4.7.6 Banner image URL mapping

You may define URL mappings for the head banner image and the foot banner image. The following attributes are allowed with the `<area>` tag:

```
shape="rect|circle|poly|point"  
coords="x1,y1,x2,y2"  
href="URL"  
alt="Alternative text"*  
title="Tooltip text"  
target="_blank|_parent|_self|_top"**
```

- * This attribute is compulsory
- ** Only “_blank” makes sense

For further information on URL image mapping see:

www.w3.org/TR/html4/struct/objects.html#h-13.6

- In the “<branding name>” folder, open “head.map” and “foot.map” respectively and replace the default content with the `<area>` tag and the desired attributes.

Example:

```
<area
shape="rect "
coords="0,0,68,68"
href="http://www.helios.de/"
alt="HELIOS Homepage"
title="HELIOS Homepage"
target="_blank">
```

Note: You may define various URL mappings. For this, arrange the `<area>` tags one after the other.

- On the “Branding Editor” page click the “Import Brandings from WebShare File Server.” link to make your changes active.

4.7.7 Add custom banner text

You may also add custom banner text which will be included above the WebShare file browser view.

- Save your custom banner text to a file named “.wsbanner” in the desired directory, and WebShare will add this text to the file browser view.

If the “.wsbanner” file is saved to the root directory of a sharepoint, it will apply to the entire directory tree. Simple HTML tags can be used to format the text.

4.7.8 Customize brandings via CSS

If existing, the file “additional.css” in the branding folder “var/settings/WebShare/Brandings/<branding name>” will automatically be included in every WebShare server response for the corresponding branding.

As a starting point, you can use the example file “additional_samples.css”. By default, it is copied to “var/settings/WebShare/Brandings/default” during the WebShare installation. It lists ID and class names for GUI components, e.g. buttons and tables used in WebShare, and some CSS examples for customizing a branding.

Do the following to customize a branding:

- Copy “additional_samples.css” to the desired branding subfolder and edit it, or create a new UTF-8 encoded text file. In any way, save it as “additional.css”.
- Add custom style definitions to this file.
- On the WebShare “Branding Editor” page click on the “Import Brandings from WebShare File Server.” link.

Changes become visible immediately after the import, for all sessions that use the modified branding.

Examples

Use *mouse over* effect (table row background color) in the file browser:

```
.fbTable tr:hover td {  
    background-color: #CDF;  
}
```

Hide the border of file items in gallery view and show it on *mouse over*:

```
.fbGalleryView .fileItem {
    border: 1px solid transparent;
}
.fbGalleryView .fileItem:hover {
    border: 1px solid #AAA;
}
```

Align images vertically centered in gallery view:

```
.fbGalleryView .imageCell {
    vertical-align: middle;
    display: table-cell !important;
}
```

Add a black border and a checkerboard background to the image in proof mode (the PNG image must be available in the respective branding folder):

```
#screenProofImage {
    border: 1px solid #000;
    background: url(checkerboard.png) repeat;
}
```

Hide the Administration toolbar button (*Important: This does NOT disable the administration, only the accessibility from the toolbar!*):

```
#tbBAdministration {
    display: none;
}
```

Apply red and bolded text style to the Logout toolbar button caption:

```
#tbBLogout span {
    font-weight: bold;
    color: red;
}
```

Include an image to the login page, as seen in Fig. 4.19:

```
#loginImage {
    background: transparent url(helios.png) no-repeat scroll 50%;
    height: 130px;
    width: 100%;
}
```

For more examples and detailed information about used CSS IDs and class names in WebShare, see the file “additional_samples.css” in the respective branding folder. For further information about *Cascading Style Sheets* refer to: www.w3.org/Style/CSS/.

4.7.9 Customize brandings via JavaScript

If existing, the file “additional.js” in the branding folder “var/settings/WebShare/Brandings/<branding name>” will automatically be included in every WebShare server response for the corresponding branding.

As a starting point, you can use the example file “additional_samples.js”. By default, it is copied to “var/settings/WebShare/Brandings/default” during the WebShare installation. It contains information and examples about using JavaScript to customize the behavior and adding custom functionalities to a WebShare branding.

Do the following to customize a branding via JavaScript:

- Copy “additional_samples.js” to the desired branding subfolder and edit it, or create a new UTF-8 encoded text file and add custom JavaScript code to this file. In any way, save it as or rename it to “additional.js”.
- On the WebShare “Branding Editor” page click on the “Import Brandings from WebShare File Server.” link.

The script becomes active immediately after the import, for all sessions that use the modified branding.

4.7.10 Custom toolbar icons

It is possible to replace the toolbar icons that are shipped with WebShare with your custom icons:

- Create your custom icon files in one or more of the sizes, specified in the `Icon Size` pop-up menu in the “Toolbar Buttons” section (compare Fig. 4.17), and save them in PNG, GIF or JPEG format. Make sure that the icon files have the extension `.png`, `.gif`, `.jpeg` or `.jpg`.

The custom icon files must have the same base name as the icons that you wish to replace, e.g. to replace the toolbar icon “copy.png” your custom icon must be named “copy.png”, “copy.gif” or “copy.jpg”. Please do not forget to also replace the corresponding rollover icons which always have “_active” appended to their name, e.g. “copy_active.png”.

The icons shipped with WebShare are stored in “var/settings/WebShare/Brandings/default/icons”.

Note: Custom icons can be smaller than the original icons. Larger custom icon files will be clipped.

- Copy the icons into the “icons” subfolder of “var/settings/WebShare/Brandings/<branding name>”.
- On the WebShare “Branding Editor” page click on the “`Import Brandings from WebShare File Server.`” link.

The custom toolbar icons should now have replaced the corresponding icons that were selected in the “Toolbar Buttons” section.

4.7.11 Custom actions icons

It is also possible to add custom icons to those action scripts that are available in the toolbar `Actions >` menu (see **Actions >** in 6.3.1 “The WebShare toolbar”). These icons must be of the PNG format:

- Copy the icon into the “actions” subfolder (create if necessary) of “var/settings/WebShare/Brandings/<branding name>”. The custom icon must have the same name as the action script that you wish to assign the icon to, e.g. name the icon “wssendmsg.png” if you want to assign this icon to the script “wssendmsg.pl”.
- On the WebShare “Branding Editor” page click on the “`Import Brandings from WebShare File Server.`” link. The action in the `Actions >` menu should now have an associated icon.

4.8 Java Server Statistics

The “Java Server Statistics” page (Fig. 4.21) is organized in three sections: `WebShare Server Information`, `WebShare Java Information`, and `WebShare User Statistics`.

Home Refresh Administration Logout

Java Server Statistics

WebShare Server Information

Hostname: ankh.helios.de
Started at: 12:12:24 on Tue, Jan 27 2020 Europe/Berlin
Uptime: 0 days, 1 hours, 9 minutes, 58 seconds
Total HTTP transactions: 46
Average HTTP transactions time: 0.629
Total Upload: 0 kB
Total Download: 0 kB
Total Preview: 0 kB

WebShare Java Information

Vendor: [Apple Inc.](#)
Java version: 1.6.0_65
Operating system: Mac OS X 10.9.5 x86_64
Java Threads running: 37
Java memory assigned: 33 MB
Java memory available: 18 MB (18444744 bytes) [Free memory](#)

WebShare User Statistics

Active users: 2
Peak active users: 2
Peak active users at: 12:21:51 on Tue, Jan 27 2020 Europe/Berlin
Session details: [Show](#)

Fig. 4.21: WebShare “Java Server Statistics” page

4.8.1 WebShare Server Information

This section contains general information about the WebShare Web Server, such as the host name, the server start time, the uptime, the number of HTTP transactions and the average time per HTTP transaction, i.e. the elapsed time between HTTP request and response. In addition, the total amounts of uploaded, downloaded and previewed data are displayed.

4.8.2 WebShare Java Information

Provides information on the hardware vendor, the OS, the Java version, the number of active Java threads, and the assigned and available memory. Clicking on the `Free memory` link frees allocated memory that is currently unused.

4.8.3 WebShare User Statistics

Provides information about currently active and peak active users. You can view session details by clicking on the `Session details: Show` link. In addition, all sessions, except for the user's own session, can be terminated by clicking on the `Terminate` link (Fig. 4.22). A click on the `Session details: Hide` link closes the session details view.

WebShare User Statistics					
Active users: 2					
Peak active users: 3					
Peak active users at: 08:33:26 Mo, Jan 27 2020 Europe/Berlin					
Session details: Hide					
WebShare Session Details					
User Name	Remote Address	Requests	Login	Last Request	
hendrik	/172.16.0.2	6	Fri 12:00	Fri 12:01	Terminate
root	/172.16.0.2	23	Fri 10:50	Fri 11:59	

Fig. 4.22: WebShare session details

4.9 HELIOS Icon Collector

HELIOS Icon Collector collects all file icons from a Windows or Mac client, to make them available to the WebShare File Server for use in the file browser.

4.9.1 Icon Collector (Windows)

On Windows, document types and programs are detected by the *Registry*.

The HELIOS Icon Collector is available on the “HELIOS Applications” volume:

- Mount the “HELIOS Applications” volume and open the “Windows > WebShare Tools” folder. Double-click the “HELIOS Icon Collector.exe” program icon.

4.9.2 Icon Collector (OS X)

On Mac, file and program icons are usually located in an Application bundle in the “Applications” folder.

The HELIOS Icon Collector is available in the “HELIOS Applications” volume:

- Mount the “HELIOS Applications” volume and open the “MacOS > WebShare Tools” folder. Double-click the “HELIOS Icon Collector” program icon.
- If desired, change the icon search path using the `Search icons in:` field.

4.9.3 Usage

- In the `Save Icons in:` field specify the path to the destination folder, where the icons are stored in the HELIOS native “.wsr” format or select it using the `Browse` button (Fig. 4.23).

Important: The destination folder must already exist!

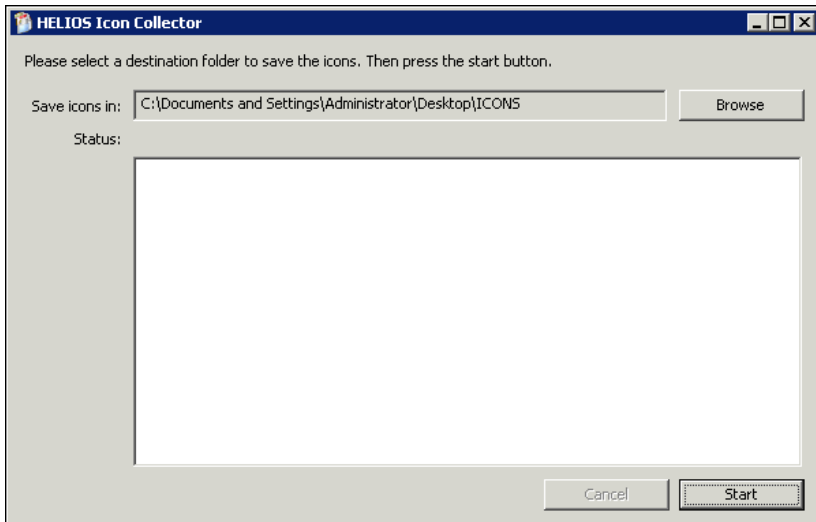


Fig. 4.23: HELIOS Icon Collector – select destination folder

➤ Click the `start` button.

The progress is shown in the window (Fig. 4.24).

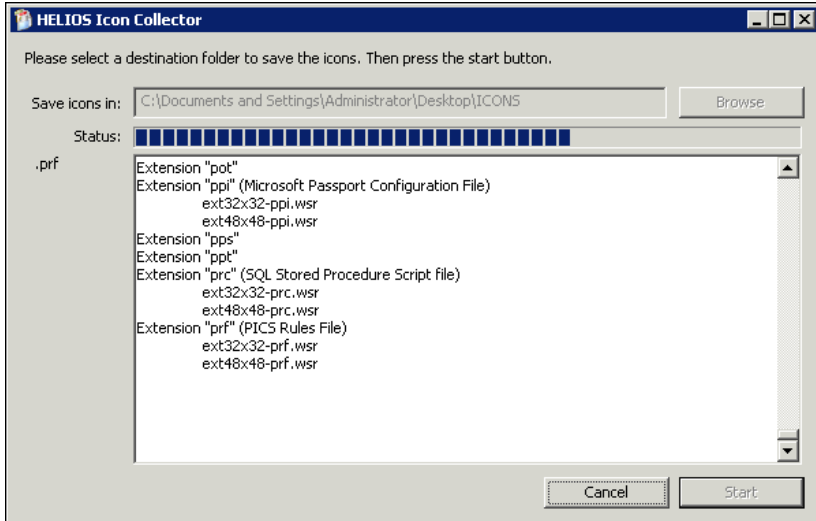


Fig. 4.24: HELIOS Icon Collector – viewing process status

The process is complete when the progress bar has reached the end. Now all available file icons are stored in the “.wsr” format in the destination folder (Fig. 4.25).

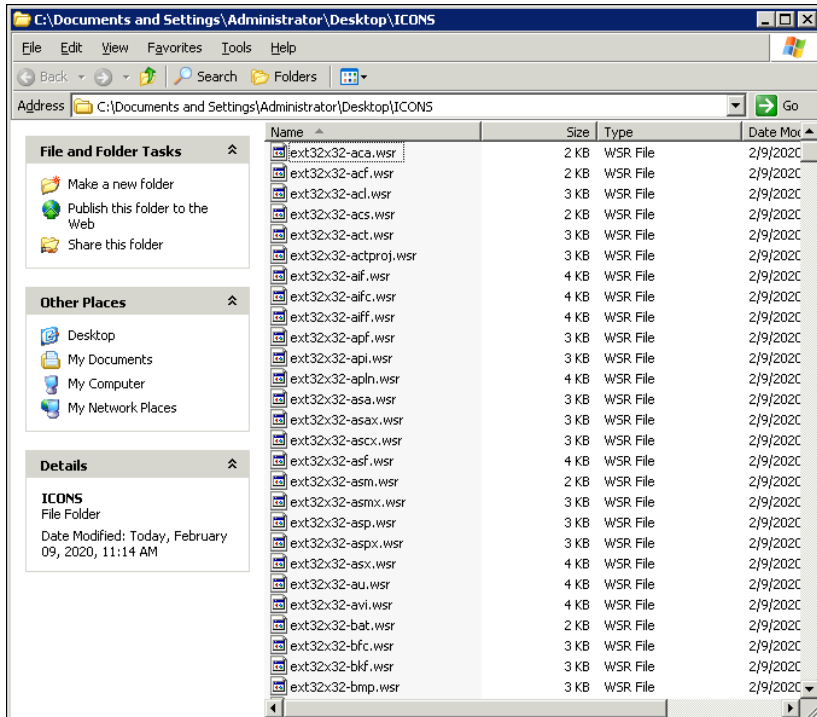


Fig. 4.25: HELIOS Icon Collector – destination folder content

The collecting of file icons can be repeated whenever new icons are added to the source workstation.

To display a “.wsr” file you can drag it in the HELIOS Icon Collector program window.

- Now copy all files to “WebShare/Icons” in the “Settings” volume on the WebShare File Server.

Custom icons

Custom icons can also be copied to the destination folder. They must have the size 32x32, 48x48 or 64x64 and be in the PNG format.

Icon names must follow a certain syntax:

- Icon by file extension

`ext<size>-<extension>`

- Icon by file type & creator

`type&creator<size>-<type (hex)>-<creator (hex)>`

- Icon by type

`type<size>-<type (hex)>`

Examples:

Sound file icon of the size 64x64 with extension “.wav”:

`ext64x64-wav.png`

Flash Player icon of the size 32x32 with type “APPL” and extension “SWF2”:

`type&creator32x32-4150504c-53574632.png`

JPEG file icon of the size 48x48 with type “JPEG”:

`type48x48-4a504547.png`

4.10 WebShare URL Share Access

WebShare URL Share Access can be used for customer convenience, to offer direct access to relevant content. Or, it can be used as part of a variable data or personalized URL system. WebShare URL Share Access offers a very powerful technology to integrate WebShare features or content into third-party or custom applications.

It allows sharing document previews or directory listings from within any text document, e-mail or web application. Single images can be referenced from HTML in the `src` attribute of an `` tag or the `data` attribute of an `<object>` tag.

The URL Share Access feature also allows sharing documents without permitting the user to navigate out of the document preview. If the `URL Document Preview only` checkbox is activated in the user configuration, the user can only access WebShare by a URL Share Access link that points to a particular document. This allows presenting PDFs and images quickly and easily without any session setup. Further customization can be done by use of additional banners. A much simpler toolbar menu will be presented in this view. Whenever possible, a `Close` button is additionally displayed (see Fig. 4.26 below).

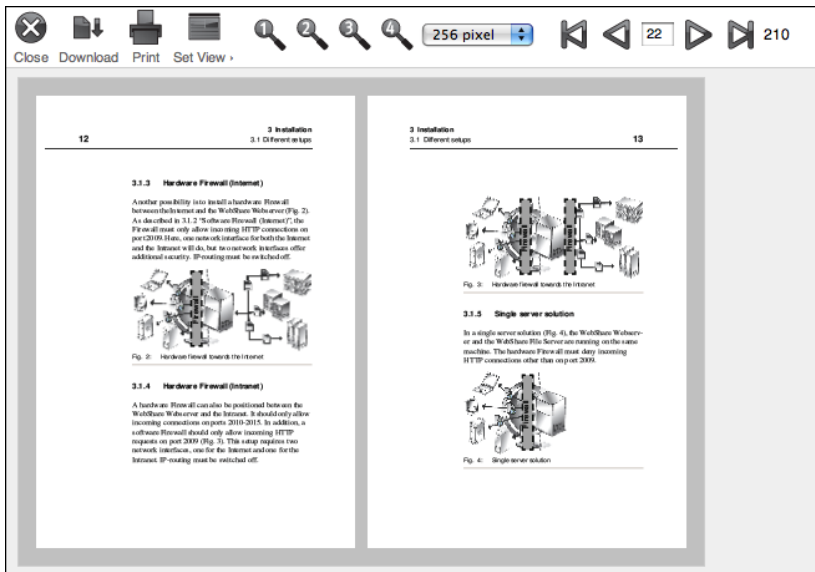


Fig. 4.26: Document opened via URL Share Access link – document preview only

4.10.1 Required parameter

server

The file server you wish to connect to, e.g.:

```
server=localhost
```

4.10.2 Login parameters

user

The user name you wish to log in with, e.g.:

```
user=webshareuser
```

password

The password for the user to log in with. If the password is omitted the user will be prompted to enter the password.

```
password=websharepassword
```

Note: To specify the `password` parameter, the `user` parameter must also be specified.

The `po` (preview only for URL Share Access) flag can be specified in the user configuration file (see 8.1 “User configuration file”) to limit a user to URL access only. This avoids that this particular user can be abused for interactive logins.

4.10.3 Path parameters

share

The sharepoint name, e.g.:

```
share=SampleImages
```


path

The path to a file or folder, e.g.:

```
path=template-images%25%30/TIFF
```

4.10.4 Image parameters

If the `path` parameter is set and points to an image file, the following parameters can be appended:

flip

Specify `h` or `horizontal` for flipping the image horizontally, `v` or `vertical` for flipping the image vertically. `hv` or `vh` or `both` flips the image horizontally and vertically. Omit this parameter or specify `none` for not flipping the image at all.

rotate

Specify `90`, `180` or `270` to rotate the image by the specified degrees. Omit this parameter or specify `none` or `0` for not rotating the image.

zoom

Specify any dpi or pixel value, e.g.: `zoom=512pixel` or `zoom=72dpi`

You may also specify comma-separated values, which are taken as `x/y` pixels, e.g.: `zoom=512,512`

If the `path` parameter is set and points to a multiple-page document the following parameters can additionally be specified:

page

Specify the desired page number of the document, e.g.: `page=3`

4.10.5 Response parameter

If the `path` parameter is set and points to an image file, you may want to fetch the image only. The following parameter can be used to embed images in an HTML page, e.g.: ``

Image-only

Specify `true` or `1` to generate a response that does just contain the requested image. Omit this parameter to get a complete WebShare session.

Important: If the `image-only` option is used PrintPreview needs to be installed on the host. Otherwise an error message is issued ("501 – Not implemented")!

4.10.6 Image only parameters

Optional parameters if `image-only` is set to `true` or `1`:

Image-type

Specify either `jpg` or `png` or `tiff` or `pdf` or `jpg2` to convert the requested image to an other file type, e.g.: `image-type=pdf`

profile

Specify the name of the ICC profile that should be applied to the image. Omit this parameter to receive the original image or specify the string `none` to have the sRGB profile applied, e.g.: `profile=MatchPrintS%201.0%20UCR-370`

Any profile listed in the `Default Simulation Profile` pop-up menu (see Fig. 6.26), or available in the HELIOS "ICC-Profiles" volume can be used as a profile name.

monitor-profile

Specify the name of a monitor profile that should be applied to the image. As a profile name any profile listed in the `Default Monitor Profile` pop-up (see Fig. 6.26) can be used, e.g.: `monitor-profile=iMac%20Calibrated.icc`

If the `profile` parameter is set to a valid ICC profile name, you may define proof color options:

filter-inks

Specify a comma-separated list of indices of each ink color that should be visible. For details refer to `FilterInks` option of the “layout” command (see HELIOS ImageServer manual), e.g.: `filter-inks=2,3,4`

4.10.7 Preview page parameters

Optional parameters if `image-only` is set to `false` or `0` and the path parameter points to a multiple-page document:

cols

Specify the number of columns that should be used for the document preview, e.g.: `cols=2`

rows

Specify the number of rows that should be used for the document preview, e.g.: `rows=4`

facing-pages

Specify `true` or `1` to enable facing pages mode. Omit this parameter or set it to `false` if you do not wish facing pages.

no-page-breaks

Specify `true`, if page breaks should be hidden. Omit this parameter or set it to `false` if page breaks should be displayed.

4.10.8 Examples

All parameters must be properly escaped (e.g. “%20” for escaping the space character).

Example 1:

Logged in as user “heliosuser” (password: “demo”) and previewing page 3 of the file “Layout.xpv” in the subdirectory “xpv_images” of the sharepoint “Sample Images”. The size is 256 pixel, rotated 90° clockwise and arranged in 2 rows and 2 columns while the pages are facing, with page breaks hidden:

```
http://ankh.helios.de:2009/app/webshare.woa/wa/linkShare?  
server=localhost  
&user=heliosuser  
&password=demo  
&share=Sample%20Images  
&path=xpv_images/Layout.xpv  
&rotate=90  
&cols=2  
&rows=2  
&facing-pages=true  
&zoom=256pixel  
&page=3  
&no-page-breaks=true
```

Example 2:

Logged in as user “heliosuser” (password: “demo”) and accessing the “default” directory in the sharepoint “Brandings”:

```
http://ankh.helios.de:2009/app/webshare.woa/wa/linkShare?  
server=localhost  
&user=heliosuser  
&password=demo  
&share=Brandings  
&path=default
```

Example 3:

Logged in as user “heliosuser” (password: “demo”) the response to the request will only be the image “Cafeteria-RGB.tif”. This allows embedding an image in a web page:

```
http://ankh.helios.de:2009/app/webshare.woa/wa/linkShare?
server=localhost
&user=heliosuser
&password=demo
&share=Demo
&path=SampleImages/TIFF/Cafeteria-RGB.tif
&image-only=1
```

In addition, an ICC profile may be applied to the image, and the image format can be converted to PDF:

```
http://ankh.helios.de:2009/app/webshare.woa/wa/linkShare?
server=localhost
&user=heliosuser
&password=demo
&share=Demo
&path=SampleImages/TIFF/Cafeteria-RGB.tif
&image-only=1
&profile=MatchPrintS%201.0%20UCR-370
&image-type=pdf
```

4.10.9 URL Share Access Helper

“URL Share Access Helper” is a convenient tool to generate URL Share Access links without the need to specify each desired parameter in the web browser’s URL address bar.

- Mount the “HELIOS Applications” volume and open the HTML file “UrlShareAccessHelper.html” from the “Documentation” folder in a web browser.
- Fill in the form fields according to your needs and finally click on *Generate Link*.

The generated link can be clicked in order to log in to WebShare with the specified parameters.

4.10.10 Security considerations

You should give some thoughts about the security when using WebShare URL Share Access:

- Access data (user name and password) are stated in cleartext in the browser address bar
- The option `image-only=1` can be deleted from the browser address bar in order to receive a complete session

You can do the following to reduce the security risk:

- Establish a special user who is used for URL Share Access only
- Use a user who has document preview-only access (`URL Document Preview only` option)
- Only allow that user to access specific sharepoints. Set all other sharepoints to deny that user access (`Allowed Users, Allowed Groups` in the “Sharepoint Administration” dialog).
- Establish read-only permissions for the sharepoint

4.11 WebShare catalog presentation

The WebShare catalog presentation allows presenting a multiple-page PDF document, to be displayed in a web browser with a simplified user interface. WebShare options such as Login, Sharepoints, Administration are invisible and therefore unavailable for the user. Depending on the permissions, the user can view a PDF document in multiple zooming steps, switch between pages, print the current document view, and download the document. This makes it very easy to provide versions of a PDF catalog. Remote users simply click on a given URL, which then opens the catalog presentation.

The WebShare catalog presentation uses the *URL Share Access* feature (see 4.10 “WebShare URL Share Access”). “UrlShareAccessHelper.html”, an HTML page, which is available in the “HELIOS Applications” volume, helps generate a static URL that can be used for remote users to access the catalog presentation. The remote user is in a kind of sandbox and does not see other WebShare options, only the PDF file will be presented.

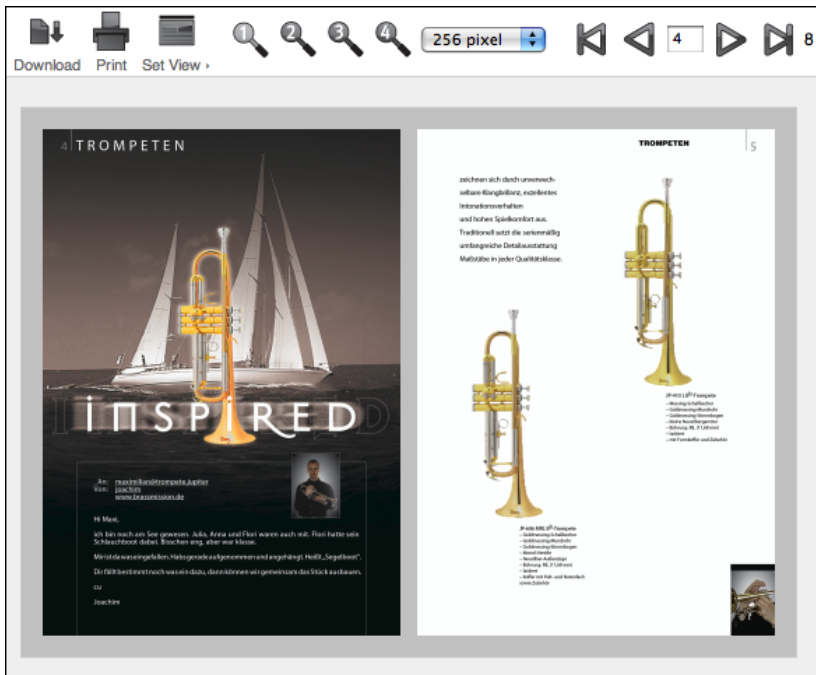


Fig. 4.27: WebShare catalog presentation sample

The catalog presentation interface can also be customized by using a custom branding. Additional HTML banner and trailer files allow placing some

additional text information on the top and bottom of the PDF document, e.g. advertisements and other important information.

Steps to set up the WebShare catalog presentation:

Step 1 – WebShare User Administration

- Create a new user or use an existing one that should be the user which runs for all catalog clients. Check the `URL Document Preview only` option for this user. This means that the user cannot login interactively, this user is forced to run the simplified presentation mode only.

Step 2 – Create the URL for the catalog presentation

- Open the “UrlShareAccessHelper.html” file in a browser. Specify the server, username, file path, etc. settings (check 4.10 “WebShare URL Share Access” for details).

Optional steps

- Customize a branding and assign this branding to the user you created in “Step1” (see 4.3 “User Administration”).
- Add an HTML banner and trailer file. These HTML files must be in the same directory where the PDF file is stored. The HTML banner uses the document name with the suffix “.banner”, e.g. “Document1.pdf.banner”, the trailer HTML uses the suffix “.trailer”, e.g. “Document1.pdf.trailer”.

Distribute the generated URL to remote users who should be allowed access to this document. Depending on the access rights, they may also download the document. It is very easy for remote catalog users because they do not need any user credentials, nor do they see any other WebShare data.

This feature allows making this print catalog quickly available to remote users, reducing printing and making intermediate versions available via WebShare catalog presentations only.

4.12 Troubleshooting

Wrong Java version on WebShare Web Server

The WebShare Web Server needs Java 6 or newer (64-bit). Older versions produce some “Class not found” errors, which do not identify the problem.

Solution:

Install a newer Java version for your WebShare Web Server.

Please make sure that Java is found when “start-helios” is issued. A symbolic link from your Java runtime to “/usr/bin/java” could be a solution. The Java version can be verified with the command:

```
# java -version
java version "1.6.0_38"
Java(TM) SE Runtime Environment (build 1.6.0_38-b05)
Java HotSpot(TM) Client VM (build 20.13-b02, mixed mode, sharing)
```

Custom file icons do not appear after an upload

Many browsers only support the data fork for the upload. This means that additional information like a custom icon, the correct Type & Creator, etc. gets lost during the upload.

Solution:

Create a Zip archive using the OS X Finder Zip utilities, which will include all metadata and WebShare will correctly unpack it on the server. A second benefit is that Zip archives are smaller.

Note: Custom icon support requires EtherShare or PCShare.

Uploading file names with special characters contain wrong file names after the upload

All major browsers support UTF-8 web pages, unfortunately some fail to accept/preserve file names in upload forms with umlauts, etc.

Solution:

Create a Zip archive and upload the archive. OS X Finder Zip and Windows Zip include correct file names which will be unpacked correctly on the server by WebShare.

No icons after file upload in WebShare sharepoint window

Files are displayed with a generic icon instead of the application or document icon in the sharepoint window.

Solution:

First, verify that the sharepoint corresponds to or is contained within a HELIOS volume. See 4.5 “Sharepoint Administration”.

Then use the HELIOS Icon Collector (4.9 “HELIOS Icon Collector”) to collect the icons on a client and copy them to the WebShare server.

Missing response for long directory listings

If a long directory listing is requested (e.g. more than 4000 files) and no response is received by the client this can be caused by a memory bottleneck. Check the “websharewoa.log” file in “HELIOSDIR/var/adm” for a message like the following WebObjects error message:

```
[2007-11-07 09:00:14 CET] <WorkerThread3> <WOWorkerThread id=3
socket=null>
Throwable occurred: java.lang.OutOfMemoryError
```

Solution:

Allocate more memory to the “websharewoa” process by using the preference:

```
# prefvalue -k Programs/websharewoa/JavaOptions -t strlist
-- "-Xms[MIN_SIZE_IN_MB]m,-Xmx[MAX_SIZE_IN_MB]m"
```

`MIN_SIZE_IN_MB` specifies the initial size of the Java memory allocation pool, while `MAX_SIZE_IN_MB` specifies the maximum size of the Java memory allocation pool.

`MIN_SIZE_IN_MB` must be greater than 1 MB, `MAX_SIZE_IN_MB` must be greater than 2 MB, e.g.:

```
# prefvalue -k Programs/websharewoa/JavaOptions -t strlist
-- "-Xms32m,-Xmx512m"
```

Default for `MIN_SIZE_IN_MB`: “32m”; for `MAX_SIZE_IN_MB`: “128m”.

WebShare login with “WebShare File Server” set to “localhost” can fail

If an error message like: `Cannot connect to server: java.io.IOException: Socket connect to localhost failed, error: Connection refused` is returned, the server is set up to use IPv6.

Solution:

Instead of using “localhost” you can use either the IPv4 number of “localhost” (127.0.0.1), the real host name of the server (e.g. “mywebshare-server”) or with its DNS name (e.g. “mywebshareserver.mycompany.com”).

Another option would be to specify “WSHostName” for the WebShareWOA server, so that the “WebShare File Server” field contains that name by default, instead of “localhost”.

You can set this preference by means of the “prefvalue” command:

```
# cd /usr/local/helios
# bin/prefvalue -k 'Programs/websharewoa/WSHostName' -t str
"mywebshareserver"
```

Thereafter, a stop/start of “websharewoa” is required to activate that change:

```
# bin/srvutil stop websharewoa
# bin/srvutil start websharewoa
```

Another option could be to specify a Java preference so that the Java engine does prefer the IPv4 stack:

```
# bin/prefvalue -k  
  'Programs/websharewoa/java.net.preferIPv4Stack' -t bool TRUE
```

Again, a stop/start of “websharewoa” is required to activate that change.

4.12.1 Limitations

Due to internal limits, WebShare cannot select more than 4096 items, for deleting, downloading, etc.

Solution A:

Select a parent folder.

Solution B:

Select smaller chunks.

5 HELIOS Admin

In addition to the web-based administration (see previous chapter 4 “Administration”), WebShare users and sharepoints can be configured and administered from within HELIOS Admin. This administration service is comprised of two components, the HELIOS Admin server and the HELIOS Admin client.

The HELIOS Admin client is a convenient tool that allows configuring users, groups, volumes and sharepoints, printer queues, etc., and which is supported for various client platforms, due to its Java heritage. For details see the chapter “HELIOS Admin” in the HELIOS Base manual.

In this manual we focus on the WebShare related usage of HELIOS Admin, such as configuring WebShare users and sharepoints.

5.1 General remarks

This chapter describes the use of the application HELIOS Admin to perform WebShare related configuration from any workstation in a convenient and secure way.

In order to use HELIOS Admin, the HELIOS Admin server must already be running on the host you want to configure. The HELIOS Service Controller is configured to start this service automatically when the system is booted.

Other chapters in this manual describe how administrative work, which is required to configure and maintain the WebShare system, can be done directly on the host, e.g. by using “prefvalue” (see “HELIOS utility programs” in the

HELIOS Base manual). However, most of these tasks can be carried out much easier using HELIOS Admin from one of the workstations.

HELIOS Admin offers a high degree of convenience to the system administrator. The application allows the host configuration to be represented graphically with lists and windows.

HELIOS Admin accesses and modifies the “Preferences” configuration file. HELIOS Admin and the HELIOS Admin server have built-in safety checks to avoid conflicting or invalid configuration settings.

HELIOS Admin has the additional advantage that almost all changes are immediately effective, without having to restart the affected service.

5.2 WebShare Server Settings

General

The `General` tab (Fig. 5.1) provides the same general options and preferences that are available in the web-based administration (Fig. 4.3 in 4.1 “Server Preferences”), where they are described.

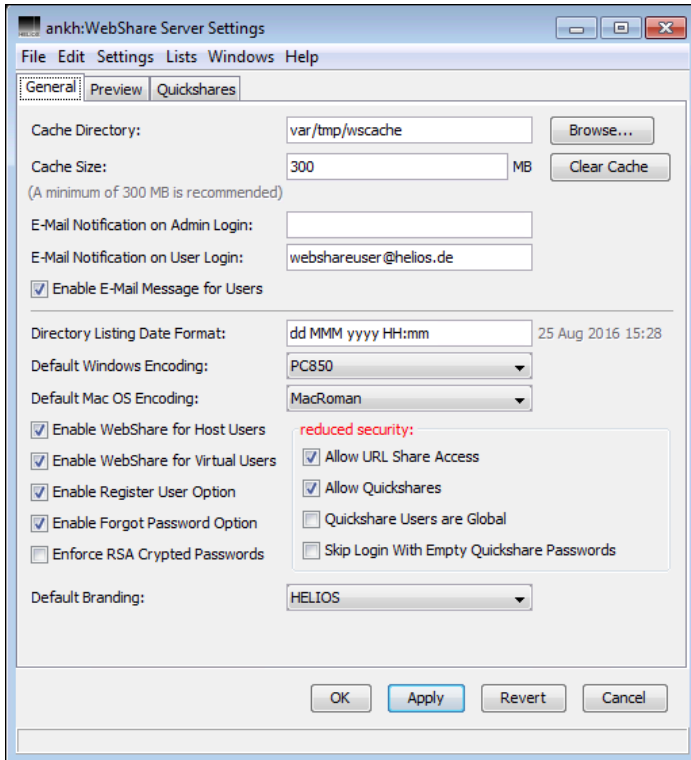


Fig. 5.1: WebShare Server Settings – General tab

Preview

Likewise, preview-related options and preferences in the `Preview` tab (Fig. 5.2) are also available in the web-based administration (Fig. 4.3). See 4.1 “Server Preferences” for a description.

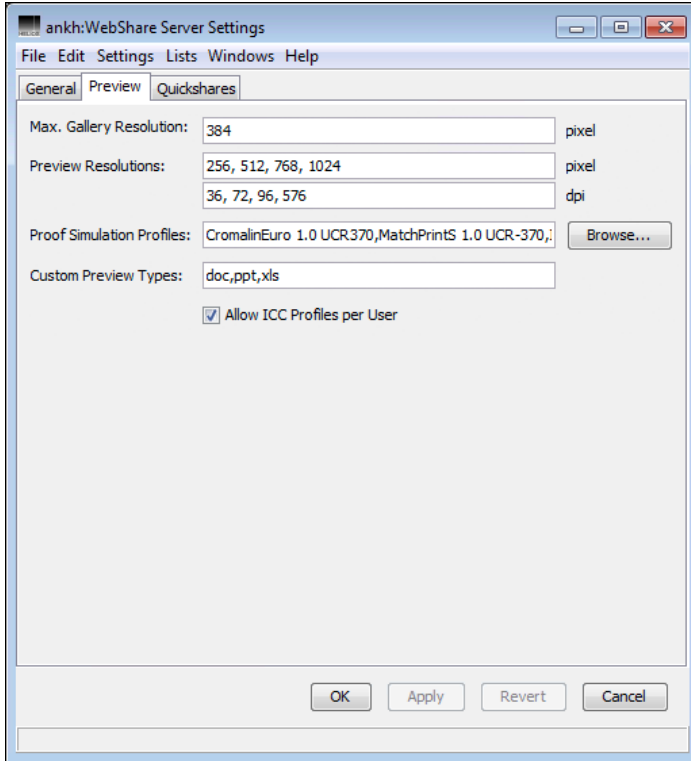


Fig. 5.2: WebShare Server Settings – Preview tab

Quickshares

The `Quickshares` tab (Fig. 5.3) lists all Quickshares that are defined on this server. This information is the same that is available in the lower part of the web-based administration window (Fig. 4.4).

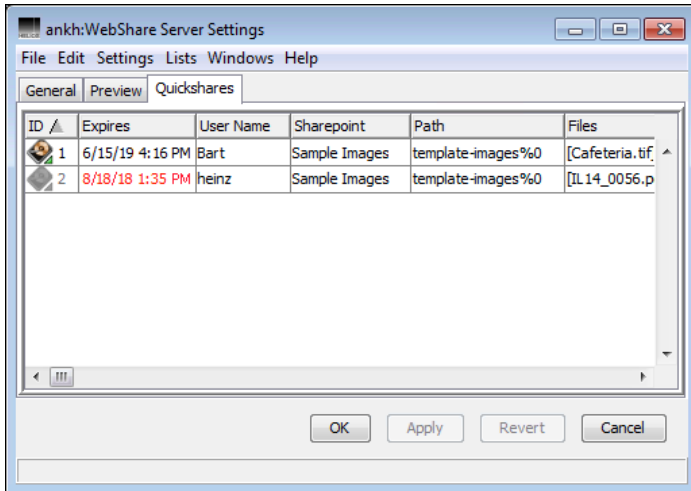


Fig. 5.3: WebShare Server Settings – Quickshares tab

A double-click on an entry opens the “Quickshare:<#>” window (Fig. 5.4). In this window, certain Quickshare information can be modified:

- The checkboxes `Active`, `Preview`, `Download`, `Upload`, `E-mail on access`
- The selection `Web Server`
- The entry fields `Expires`, `Comment`

All other fields cannot be changed but their content can be selected and copied to paste into another application, e.g. to send the URL to the e-mail address of the Quickshare user. The options are described in 4.2 “Quickshare Administration”.

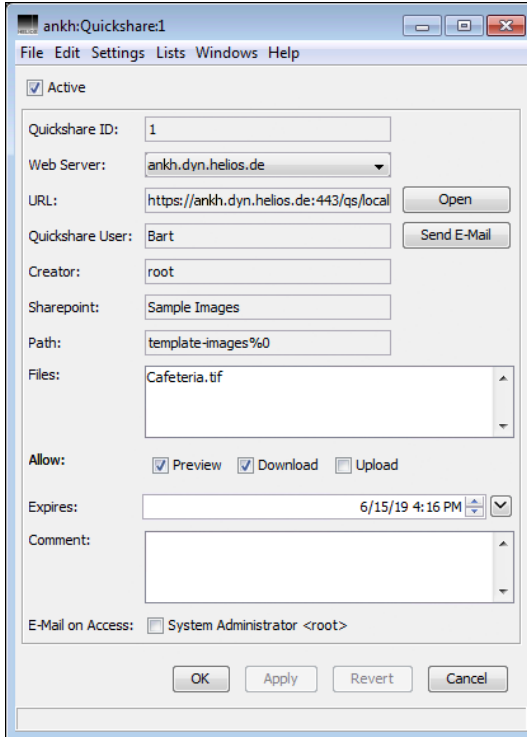


Fig. 5.4: Quickshare administration

5.3 Sharepoints

The `Sharepoints` tab shows all HELIOS WebShare sharepoints on the host (Fig. 5.5). The HELIOS Admin server automatically creates this list by inspecting sharepoint-related entries in the “Preferences” file (see 8.5.2 “Sharepoint preference keys”).

- Choose the `Sharepoints` tab. If it is not available, activate it in the `Lists` menu.

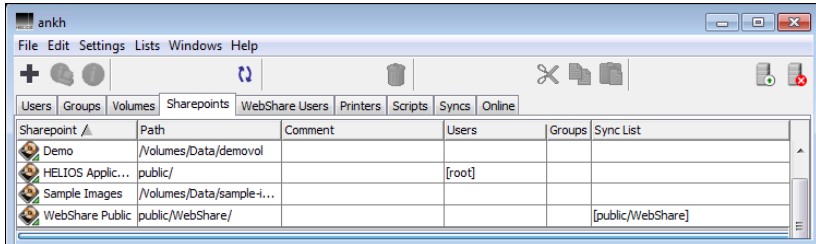


Fig. 5.5: HELIOS Admin – Sharepoints tab

- To open an entry, highlight a sharepoint name in the list and go to `File > Open`, or just double-click on the entry or press the RETURN key.

Note: For space reasons, the “Sync List” column is only displayed if at least one sync list is specified.

General

The WebShare sharepoint administration window (Fig. 5.6) in HELIOS Admin provides the same features and options that are already known from the web-based administration described in 4.5 “Sharepoint Administration” (compare Fig. 4.6).

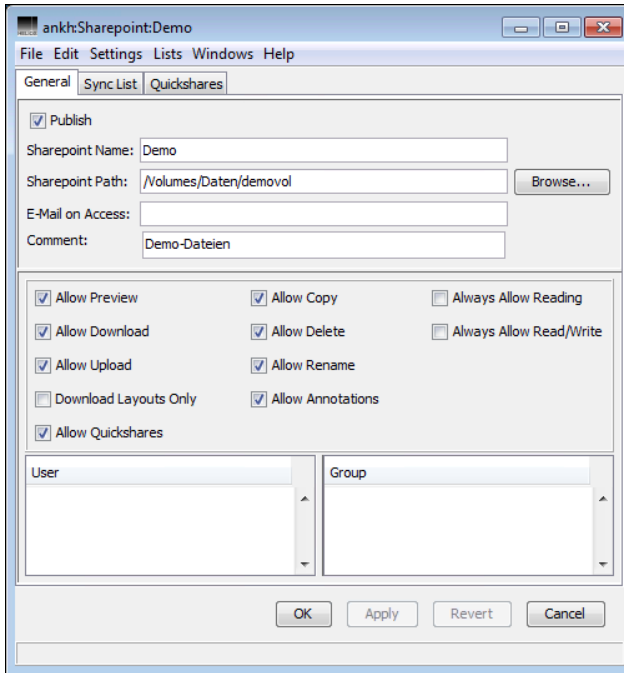


Fig. 5.6: WebShare sharepoint *General* tab

Sync List

Switching to the *Sync List* tab (Fig. 5.7), you may define files or folders in the present sharepoint that should be synchronized with a mobile device via the HELIOS Document Hub solution. See a description of the sync list feature in **Sync list** (compare Fig. 4.7).

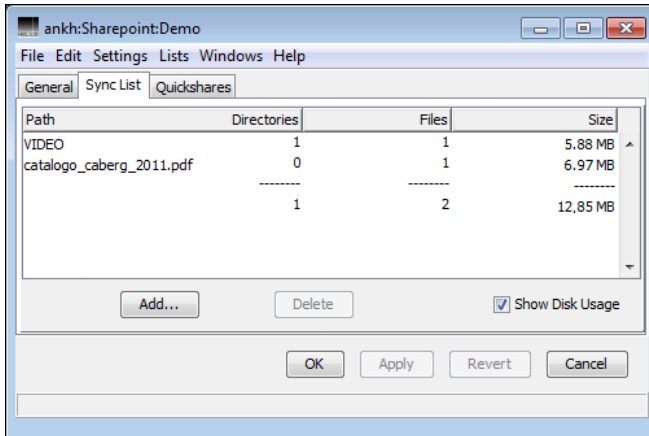


Fig. 5.7: WebShare sharepoint Sync List tab

By default, the `Show Disk Usage` checkbox is not activated. If checked, three additional columns become available: “Directories”, “Files”, and “Size” of the synchronized files.

Note: Activating the `Show Disk Usage` checkbox may slow down server performance due to the enumeration of directory trees.

Quickshares

The `Quickshares` tab Fig. 5.8 lists all Quickshares within the selected sharepoint. It contains important parts of the information that is also available in the WebShare “Quickshare Administration” window (compare Fig. 4.4 in 4.2 “Quickshare Administration”).

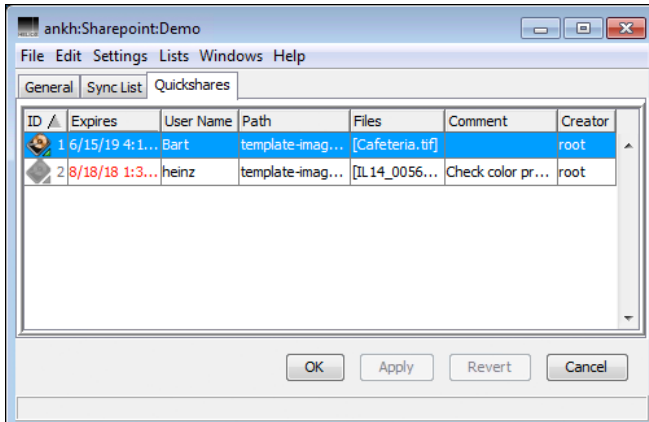


Fig. 5.8: WebShare sharepoint Quickshares tab

- To open an entry, highlight a Quickshare in the list and go to `File > Open`, or just double-click on the entry or press RETURN.

5.4 WebShare Users

The `WebShare Users` tab shows all HELIOS WebShare users on the host (Fig. 5.9). The HELIOS Admin server automatically creates this list by inspecting the “webshare.passwd” file (see 8.1 “User configuration file”).

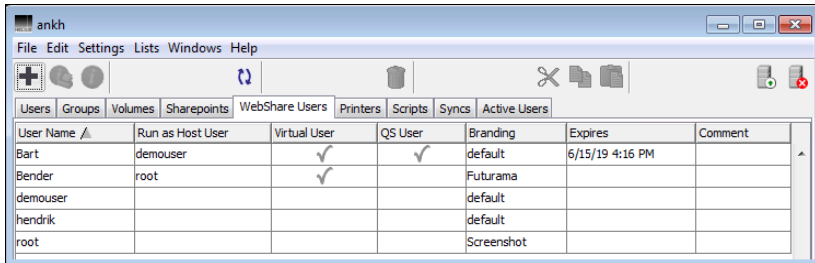


Fig. 5.9: HELIOS Admin – WebShare Users tab

- Choose the `WebShare Users` tab. If it is not available, activate it in the `Lists` menu.
- To open an entry, highlight a user name in the list and go to `File > Open`, or just double-click on the entry or press `RETURN`.

General

The WebShare user administration window (Fig. 5.10) in HELIOS Admin provides the same features and options that are already known from the web-based administration described in 4.3 “User Administration” (compare Fig. 4.5).

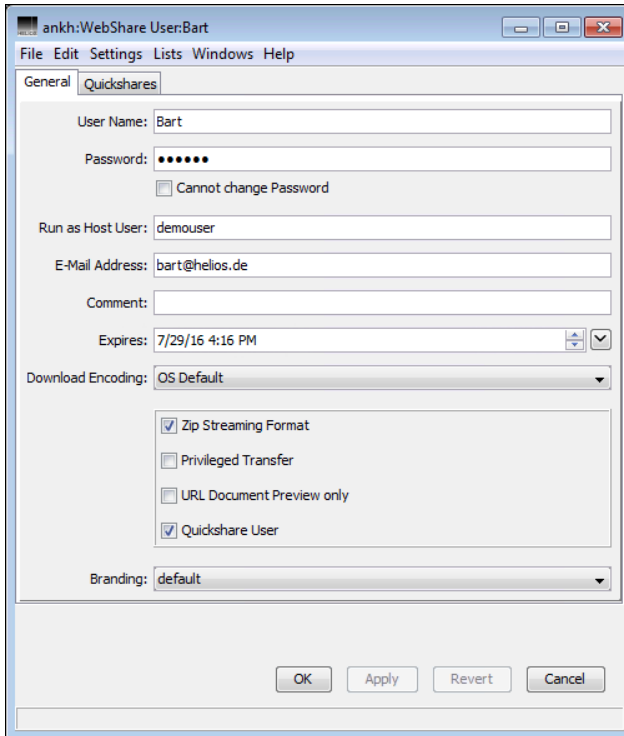


Fig. 5.10: WebShare user `General` tab

Quickshares

If one or more Quickshares have been assigned to a WebShare user, the additional `Quickshares` tab becomes available (Fig. 5.11). See a description of the Quickshares feature in 4.2 “Quickshare Administration” (compare Fig. 4.4).

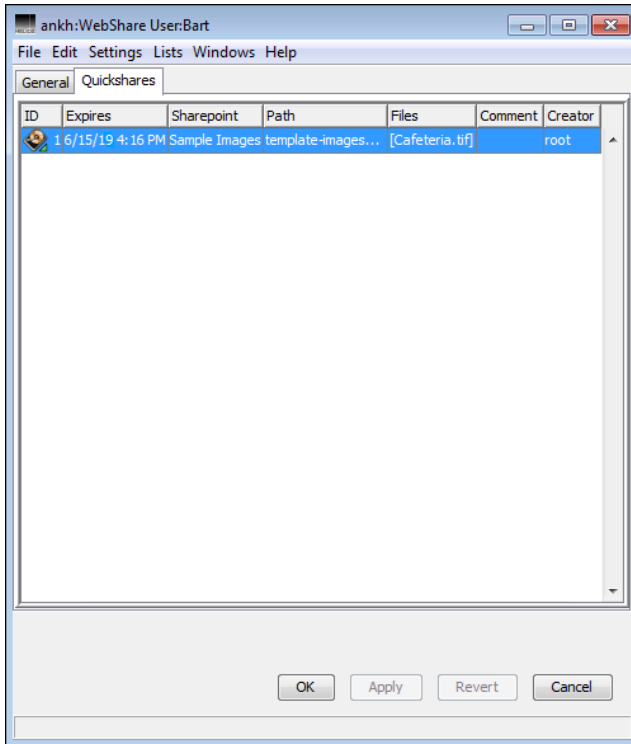


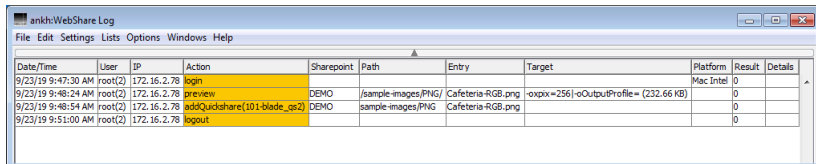
Fig. 5.11: WebShare user Quickshares tab

5.5 WebShare log file

The WebShare log file contains all details for several WebShare actions, such as login, preview, add files, delete files, etc.

The exact WebShare status codes are detailed in C “Technical notes”.

- Select `WebShare Log Files` from the `Lists` menu and specify the desired day.



The screenshot shows a window titled "ankh:WebShare Log" with a menu bar (File, Edit, Settings, Lists, Options, Windows, Help) and a toolbar. Below is a table with columns: Date/Time, User, IP, Action, Sharepoint, Path, Entry, Target, Platform, Result, and Details. The first three rows are highlighted in yellow.

Date/Time	User	IP	Action	Sharepoint	Path	Entry	Target	Platform	Result	Details
9/23/19 9:47:30 AM	root(2)	172.16.2.78	login					Mac Intel	0	
9/23/19 9:48:24 AM	root(2)	172.16.2.78	preview	DEMO	/sample-images/PNG/ Cafeteria-RGB.png		-o:pix=2561-o:OutputProfile= (232.66 KB)		0	
9/23/19 9:48:54 AM	root(2)	172.16.2.78	addQuickshare(101-blade_or2)	DEMO	sample-images/PNG	Cafeteria-RGB.png			0	
9/23/19 9:51:00 AM	root(2)	172.16.2.78	logout						0	

Fig. 5.12: Example of a WebShare log file

- Choose `Save as...` from the `File` menu to save the WebShare log file as a text file.

Note: If the filter option is active (see “Filtering log entries” in the HELIOS Base manual section below), only the filtered part of the WebShare log file is saved.

You can then read this information into a word processor for further use. HELIOS Admin gets its information from the files “HELIOSDIR/var/adm/webshare.acct” (data of “Today”) to “HELIOSDIR/var/adm/webshare.acct.6” (“7 Days Ago”). See C “Technical notes” for more information.

6 Using WebShare

This chapter explains step by step how to log on to the WebShare File Server, how to select a sharepoint and how to use the buttons in the sharepoint toolbar.

6.1 WebShare File Server login

- Launch a browser and enter the WebShare Web Server address using port 2009, e.g.: **http://hostname.company.com:2009**
- In the `WebShare File Server` field enter the name of the server you want to connect to (or just accept the provided server name), select the desired language from the `Language` pop-up menu, and click on the `Continue` button (Fig. 6.1).

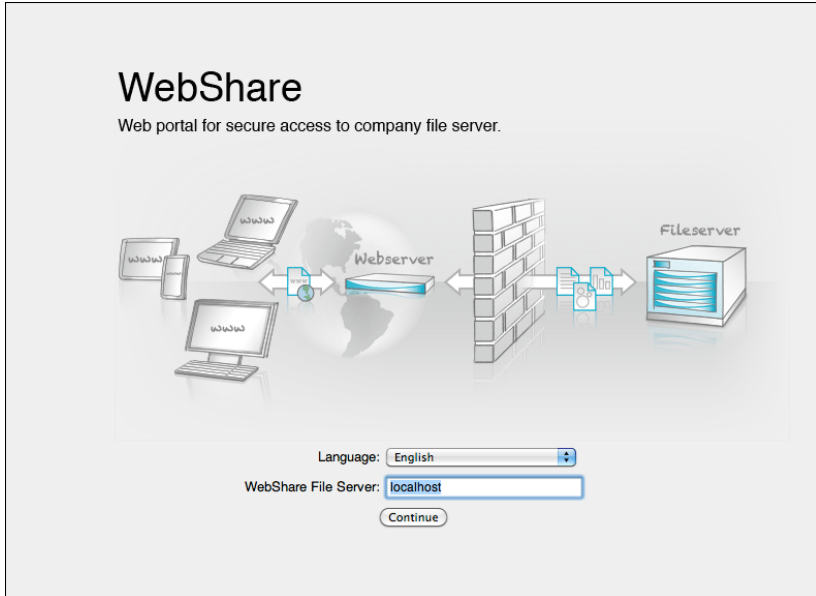


Fig. 6.1: WebShare login window

Note: The login form must be completed within 2 minutes. Otherwise a time-out error will occur. In addition, the user has only 3 trials to log in.

You may also preselect the WebShare File Server via the URL parameters “wshost” and “autoforward”:

wshost

```
http://<domain>:<port>/?wshost=<a fileserver name>
```

The file server name is set to the value specified by the “wshost” parameter in the WebShare File Server login field.

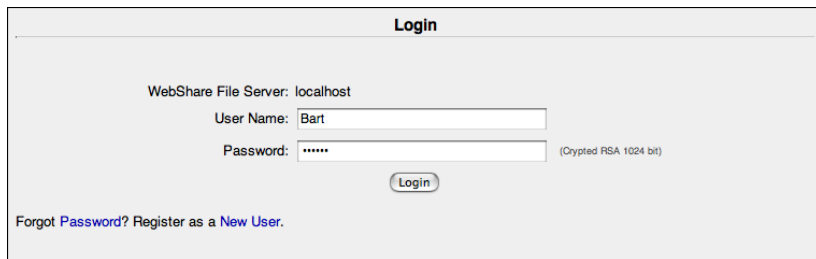
autoforward

```
http://<domain>:<port>/?wshost=<a_fileserver_name>&autoforward
```

This URL pastes the WebShare File Server name, which is handed over by “wshost”, into the WebShare File Server login field and proceeds with Continue.

For this to work, JavaScript must be activated in your browser. If JavaScript is not active, only the WebShare File Server is pasted.

- In the upcoming window fill in the User Name and Password fields and click on the Login button (Fig. 6.2).



The screenshot shows a web browser window titled "Login". The main content area has a light gray background. At the top, it says "WebShare File Server: localhost". Below that, there are two input fields: "User Name:" with the text "Bart" entered, and "Password:" with masked characters "*****". To the right of the password field, it says "(Crypted RSA 1024 bit)". Below the input fields is a "Login" button. At the bottom left, there are two links: "Forgot Password?" and "Register as a New User".

Fig. 6.2: WebShare login window

Note: The password field should have the annotation `Crypted RSA...` in order to ensure a secure password transfer. If it shows `Cleartext`, enable JavaScript in your browser to avoid insecure clear text password transfer. See also **JavaScript** in 10.1.1 “WebShare Web Server”.

If you do not already have a user name and password, use the `Register as a New User` link (if available) to enter user data in order to receive a WebShare account. If you already have a WebShare user name, but forgot your password, use the `Forgot Password?` link (if available) to request a new login password.

After a successful login, the “Home” page appears, which allows the selection of a WebShare sharepoint from the `Sharepoint Name` list (Fig. 6.3).



Fig. 6.3: WebShare “Home” page

- To open the desired WebShare sharepoint (Fig. 6.4), click on the corresponding link.

You can also open a new window for browsing by clicking on the `New` link in the “Window” column. Note that you can only have one window open for each sharepoint per login.

If you logout from one window, all other windows belonging to the same session will also be disconnected. When you then click on a link in one of these windows, you will be redirected to a “Session time out” error page with the message: `Your session has been terminated. Use the link Click here to log in again.`

6.2 WebShare access keys

WebShare supports access key navigation that facilitates many user operations, which would have been done via mouse clicks otherwise.

Access keys are enabled in a different way with different browsers. So please check your browser documentation. Access keys that are marked with an * are used without *modifier key*.

Browser	Mac	Windows
Chrome	Ctrl-Alt	Alt
Firefox	Ctrl-Alt	Alt-Shift
Internet Explorer	n/a	Alt
Safari	Ctrl-Alt	Alt

Table 6.1: Modifier keys of some browsers

A	Select/deselect all files
B	Back/Up one level
C	Copy selected files
V	Paste selected files
U	Upload
H	Home
R	Refresh current web page with latest server content
Q	Log out
P	Previous item in search/preview
N	Next item in search/preview
F	Find (in file browser) / Full-screen (in preview/proof mode)
<...*	Show previous page (in preview/proof mode)
...>*	Show next page (in preview/proof mode)

- 1 Zoom level 1 (in preview and proof mode only)
- 2 Zoom level 2 (in preview and proof mode only)
- 3 Zoom level 3 (in preview and proof mode only)
- 4 Zoom level 4 (in preview and proof mode only)
- 5 Zoom level 5 (in proof mode only; *fixed*)
- 6 Zoom level 6 (in proof mode only; *fixed*)
- 7 Zoom level 7 (in proof mode only; *fixed*)
- 8 Zoom level 8 (in proof mode only; *fixed*)
- 9 Zoom level 9 (in proof mode only; *fixed*)

6.3 Work in a sharepoint

This chapter describes how to work in a WebShare sharepoint.

Keyboard navigation for file browsing

The user has the option to search for files, e.g. in very large directories, and to “scroll” them into the visible area. For example, pressing the keys “d”, “a”, and “t”, highlights all files in the directory that start with *dat*. In doing so, if the first found entry is not in the visible area, the display is automatically scrolled into the viewer’s focus.

The interval is 0.5 seconds, i.e. the maximum time span between pressing the keys “d” and “a” is half a second, otherwise “a” is considered to be the new search letter.


Contextual file menu

A contextual menu allows faster access to commands on single items in the file browser. It provides the most used commands (*Download, Preview, Proof, Slideshow, Copy, Duplicate, Delete, Rename, Permissions, Quickshare, Open*) without the need to select the file and choose the command from the menu. *Open* allows opening PDF, movies, Flash and other file types directly in the web browser.

The screenshot shows the WebShare file browser interface. At the top, there is a navigation bar with icons for Home, Refresh, Administration, File, Edit, Transfer, Actions, and Logout. A search bar labeled 'Spotlight' is on the right. Below the navigation bar, the text 'HELIOS Demo:' and '22 objects 65.64 MB, 52.51 GB free' are displayed. The main area contains a table of files with columns for Select, Name, Type, Size, Date, and C. A contextual menu is open over the file 'CafeteriaPaths.tif', listing actions: Download, Preview (17.65 MB), Proof, Slideshow (8.91 MB), Copy, Duplicate (50 bytes), Delete, Rename (8.75 MB), Permissions, Quickshare (12 KB), and Open.

Select	Name	Type	Size	Date	C
<input type="checkbox"/>	ANNO	dir		08 Jan 2015 09:34	⊞
<input type="checkbox"/>	Band.tif	tiff	1.25 MB	16 Feb 2012 13:46	⊞
<input checked="" type="checkbox"/>	CafeteriaPaths.tif	tiff	17.65 MB	04 Jun 2008 08:39	⊞
<input type="checkbox"/>	catalogo_caberg_2011.pdf	pdf	8.91 MB	25 Oct 2010 13:43	⊞
<input type="checkbox"/>	desc.txt	text	50 bytes	05 Dec 2012 13:22	⊞
<input type="checkbox"/>	dochub_d.pdf	pdf	8.75 MB	03 Dec 2012 09:56	⊞
<input type="checkbox"/>	IMG_0003.JPG	image	12 KB	11 Feb 2016 16:14	⊞
<input checked="" type="checkbox"/>	L2 Katalog Trompeten.xpv	data	2.5 MB	29 Jun 2010 08:06	⊞
<input type="checkbox"/>	LanTest-6.0.0-172.16.2.207-Flanders.log	text	495 bytes	22 Jul 2013 12:58	⊞
<input type="checkbox"/>	Mult.txt	text	430 bytes	21 Jan 2004 14:09	⊞
<input type="checkbox"/>	PDF-Check	dir		14 Oct 2013 09:46	⊞
<input type="checkbox"/>	permtest	dir		09 Jul 2014 12:53	⊞

Fig. 6.4: WebShare file browser (default view)

- To open the menu, click on the  icon, which appears when hovering over the file name. Note that a current selection will be reset when using the contextual menu.

Note: JavaScript needs to be activated in the web browser to use features such as the contextual menu or the automatical local time zone adjustment in the "Date" column.

6.3.1 The WebShare toolbar

In the following, the icons in the toolbar (Fig. 6.5) are described. Underneath the toolbar the directory level in the sharepoint is shown. You may click on a subdirectory to jump to that level. A click on the folder symbol allows you to jump one level up or back from the preview mode.

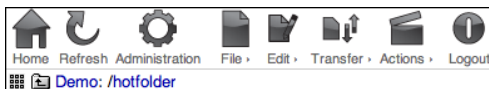


Fig. 6.5: WebShare sharepoint toolbar

Note: If items in the toolbar appear grayed out then you do not have sufficient permissions (see 4.5 "Sharepoint Administration"). Ask the Administrator.

Home

Shows a list of all sharepoints that are available to the logged-in user.

Refresh

A click on this button reloads the current page from the WebShare File Server.

Administration

Opens the WebShare “Administration” page. See Fig. 4.2 in 4 “Administration”.

File >

This toolbar item contains a submenu with the following items:

Create Dir

Create a new directory in the sharepoint.

Permissions

View and change file or folder permissions. This feature is of great value, to allow or deny other users access to files and folders. See also 6.3.3 “Note on file access permissions”.

Note: Changing permissions is only allowed if `Allow Rename` is activated (see `Allow Rename` in 4.5 “Sharepoint Administration”).

Rename

Rename a selected file or directory in the sharepoint.

Duplicate

Duplicate one or more selected files or directories into the same directory. Duplicated files will have “copy”, “copy 1”, “copy 2”, etc. appended to their name, before the suffix.

Delete

Delete the selected files from the sharepoint. As a means of security and to avoid inadvertent deletion, you will be asked to confirm the deletion by clicking on the `Remove Selected Items` button or `Cancel` to remove all checkmarks.

Preview

Show a preview of the selected item(s); if no item has been checked all suitable

documents are opened in preview mode. See also 6.4 “Image and document previews”.

Proof

Show a proof of the selected item(s); if no item has been checked all suitable documents are opened in proof mode.

Slideshow

Create a slideshow from the selected items (see Fig. 6.6); if no item has been checked all suitable documents are opened in a slideshow.

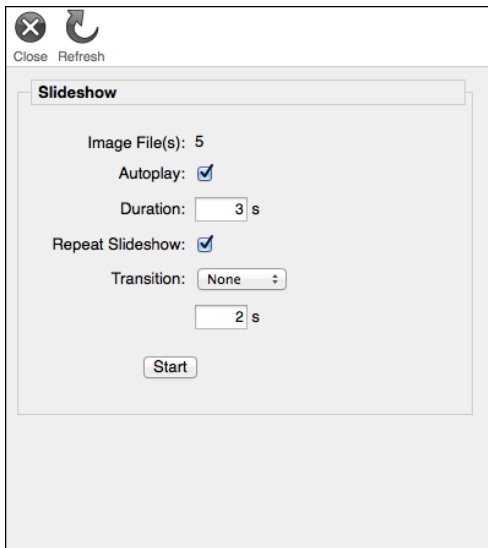


Fig. 6.6: WebShare Slideshow

Autoplay

After clicking the `Start` button the slideshow starts automatically. If this option is not selected, the slideshow will not run automatically; manual navigation is then required.

Duration

Determines the time interval in seconds between the slides change.

Repeat Slideshow

With this option enabled, the slideshow will start over again when it has reached its end.

Transition

Allows adding a transition style between the single slides. You can choose between `Fade-in` and `Slide-in`.

Navigation:

Key	Action
<code>esc</code>	Stop slideshow
<code>⏸</code>	Pause/resume slideshow
<code>⏪</code>	Previous page
<code>⏩</code>	Next page
<code>↗</code>	Next document
<code>↖</code>	Previous document

Search

Search for files and folders within the sharepoint. In the example below (Fig. 6.7) a full-text search for files with the terms “job”, “titles”, and “print” is done. You may filter the search by the modification date with the pop-up menu `Modified`, and also limit the number of hits with the `Max. Results` pop-up menu. If the `Limit Search To Current Folder` option is checked, the search is limited to the folder from which the search was started. Searches are case-insensitive.

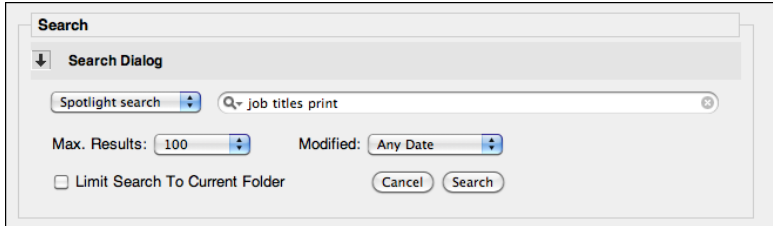


Fig. 6.7: WebShare search function

After clicking on the `Search Files` button all hits are listed in the `Search Result` section (Fig. 6.8). You may directly go to each hit by either using the arrow buttons, by clicking on the link underneath each hit or by using the access key `P` and `N` (see 6.2 “WebShare access keys”). All described ways have in common that the file is selected automatically. However, clicking on the file name itself will open the file in preview mode.

The `File Search` as well as the `Search Result` section can be hidden by clicking on the arrows in the left upper corner of the respective section or by clicking the caption “Search Dialog” and “Search Result” respectively. Another click will show them again.

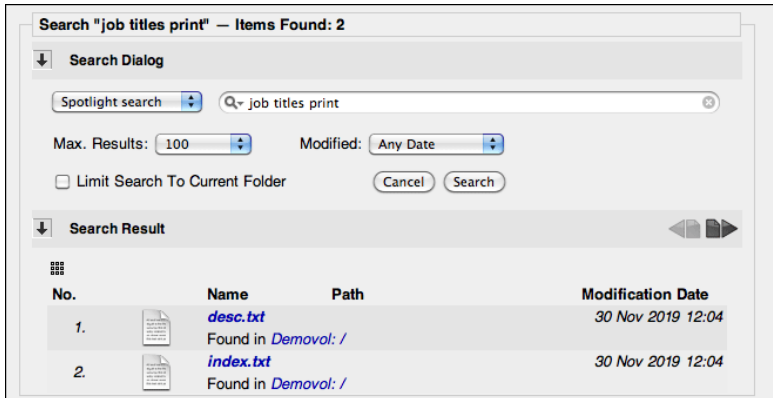


Fig. 6.8: WebShare search results

A click on the `Cancel` button will close the WebShare file search section.

More details on the HELIOS Spotlight search, and search options, are covered in the HELIOS Index Server manual, in the chapters “Simple Spotlight syntax” and “Advanced Spotlight syntax”.

When moving the cursor over the Spotlight search field in the WebShare toolbar or the “Search Dialog” search field (`Spotlight search` must be selected from the pop-up menu), a link to a Spotlight search help pop-up window becomes visible (Fig. 6.9).

The link `Show all indexed attributes`, at the bottom of the “Spotlight Help” window, displays all attributes indexed by the indexer modules for that sharepoint (see HELIOS Index Server manual). A click on an attribute inserts it in the search field.

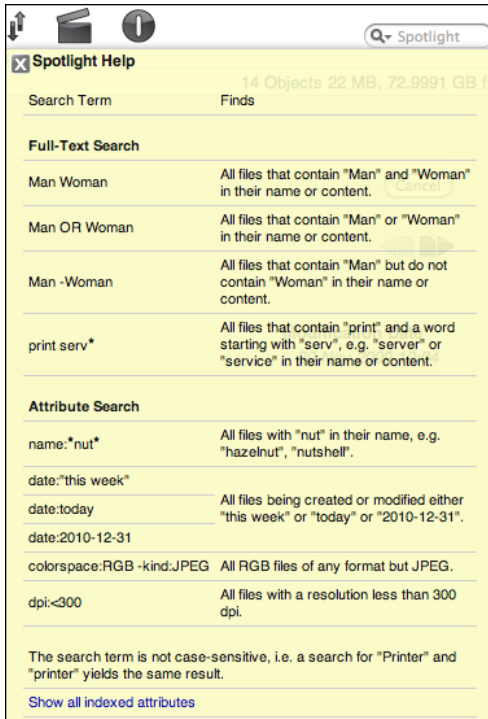


Fig. 6.9: Spotlight Help pop-up

Label >

Mac operating systems up to Mac OS 9.x, and then again from OS X 10.3 on, allow assigning color labels to files and folders. Files and folders can be “marked” for their importance or priority. HELIOS WebShare offers a similar functionality in this submenu.

Note: HELIOS Admin allows defining color labels in its `Settings > Color Labels` menu (see HELIOS Base manual).

Set View >

Change the view of the file browser, e.g. add or extend column types, and display the listing in a set of 4 predefined modes (*Default*, *Smart*, *Extended*, and *Small*). The *smart* view option displays a server-generated preview thumbnail of image files instead of the file type thumbnail. Note that only the *extended* view option includes the UNIX file permissions, which is a convenient means to see who is allowed access to specific files and folders. These permissions can be changed by using the *Permissions* option in the pop-up menu (see above). The options *Hide Comments* and *Show Comments* allow hiding and unhiding file comments.

You may also browse the files in a *gallery* view mode rather than in a list. The gallery view mode can be enabled in two ways:

➤ From the sharepoint toolbar select *File > Set View > Gallery*.

Or just click on the gallery icon (🖼️) in the toolbar, adjacent to the sharepoint path information.

Edit >

This toolbar item contains a submenu with the following items:

Select All

Mark all checkbox items in a sharepoint at the same time. Clicking on this button again will unmark all items.

Copy

Copy one or more selected files or directories into the WebShare internal clipboard for later pasting.

Paste

Paste one or more previously copied files or directories into the currently opened sharepoint directory path. Existing files are not overwritten, but will have “dup”, “dup 1”, “dup 2”, etc. appended to their name, before the suffix.

Note: The difference between copying/pasting a selection and duplicating is that copied items can be pasted into different sharepoints or different directories. However, duplication is only possible within the same sharepoint, i.e. directory.

Note: `Copy`, `Move` and `Paste` are allowed according to your server file and folder permissions within the sharepoint. The setting of the `Always Allow Reading` and `Always Allow Read/Write` checkboxes (see 4.5 “Sharepoint Administration”) has no influence on that.

Move

Move one or more previously copied files or directories into the currently opened sharepoint directory path. The behavior is the same as if using `Paste`, with the exception that the source files or directories are deleted.

Mail

WebShare provides a front-end for the HELIOS mail tool, which allows sending e-mails directly from within WebShare. Selected files and folders will be listed in the mail body (Fig. 6.10).

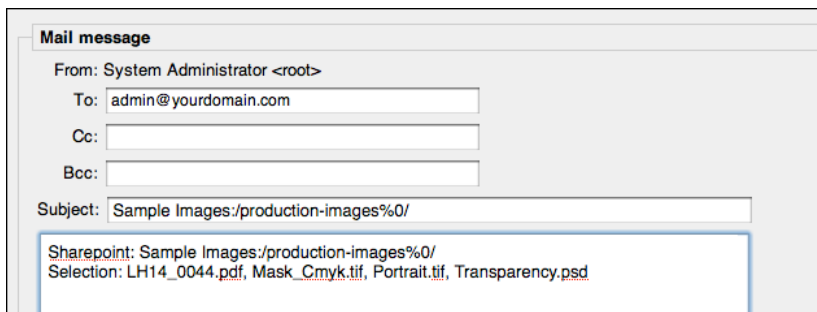


Fig. 6.10: WebShare mail functionality

Transfer >

This toolbar item contains a submenu with the following items:

Download

Download one or more files or folders that have been marked to the local disk. These will be transferred in a Zip file named “download.<date>.zip”. For example, the file “Cafeteria.tif” will be contained in a Zip file named “download.14-06-15.zip” after being downloaded from a WebShare sharepoint on June 15, 2014.

Important: Empty directories are not included in the downloaded Zip file. Color labels, comments, and other attributes are preserved for downloaded *files*, but not for *folders*.

After extraction, each download folder includes the file “DownloadLog.txt”, which contains a list of successfully downloaded items, and for any omitted items a short description why they were omitted.

Upload

In the “Upload” dialog (Fig. 6.11) you can select the file(s) to be uploaded.

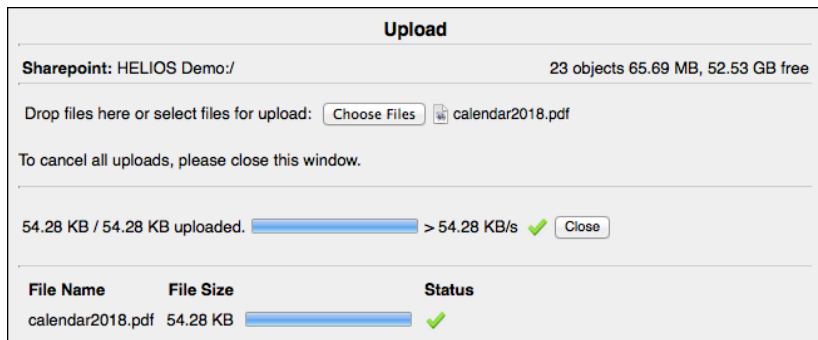
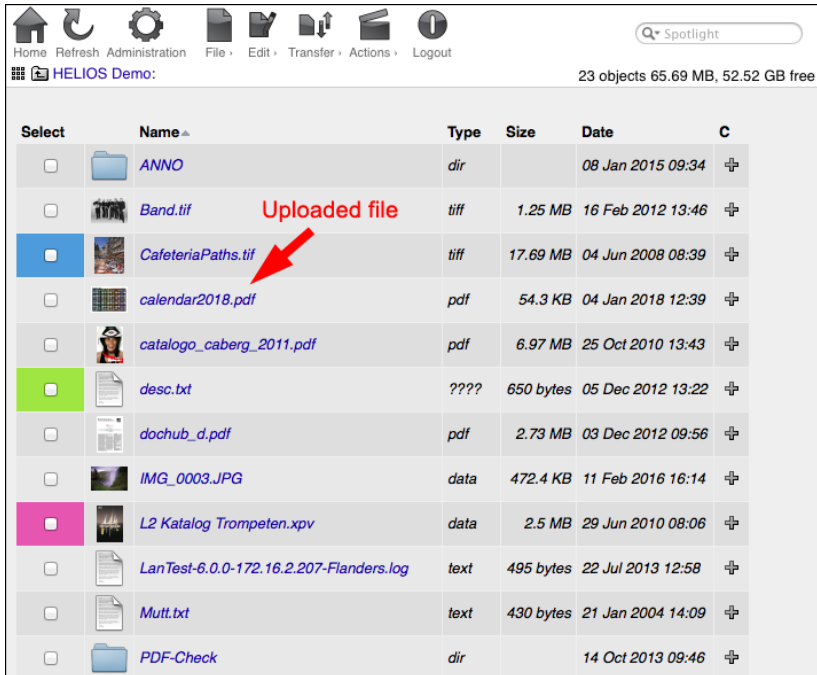


Fig. 6.11: WebShare sharepoint file upload

After being uploaded, the file(s) are listed in the current sharepoint (Fig. 6.12, compare with Fig. 6.4).



Home Refresh Administration File Edit Transfer Actions Logout

HELIOS Demo: 23 objects 65.69 MB, 52.52 GB free

Select	Name	Type	Size	Date	C
<input type="checkbox"/>	ANNO	dir		08 Jan 2015 09:34	+
<input type="checkbox"/>	Band.tif	tiff	1.25 MB	16 Feb 2012 13:46	+
<input checked="" type="checkbox"/>	CafeteriaPaths.tif	tiff	17.69 MB	04 Jun 2008 08:39	+
<input type="checkbox"/>	calendar2018.pdf	pdf	54.3 KB	04 Jan 2018 12:39	+
<input type="checkbox"/>	catalogo_caberg_2011.pdf	pdf	6.97 MB	25 Oct 2010 13:43	+
<input checked="" type="checkbox"/>	desc.txt	????	650 bytes	05 Dec 2012 13:22	+
<input type="checkbox"/>	dochub_d.pdf	pdf	2.73 MB	03 Dec 2012 09:56	+
<input type="checkbox"/>	IMG_0003.JPG	data	472.4 KB	11 Feb 2016 16:14	+
<input checked="" type="checkbox"/>	L2 Katalog Trompeten.xpv	data	2.5 MB	29 Jun 2010 08:06	+
<input type="checkbox"/>	LanTest-6.0.0-172.16.2.207-Flanders.log	text	495 bytes	22 Jul 2013 12:58	+
<input type="checkbox"/>	Mutt.txt	text	430 bytes	21 Jan 2004 14:09	+
<input type="checkbox"/>	PDF-Check	dir		14 Oct 2013 09:46	+

Fig. 6.12: WebShare uploaded file in sharepoint

When the upload is complete, details in terms of file size, upload performance, etc. are displayed.

Note: If ImageServer and WebShare are installed on the same host, and the `Create Layouts` option in HELIOS Admin is enabled for that volume, the OPI server will by default create layouts of uploaded files. You can switch this behavior off according to the instructions given in the HELIOS ImageServer manual.

If the name of a file to be uploaded already exists in the destination folder, the uploaded file will have “dup”, “dup 1”, etc. appended to its name, before the suffix. This refers only to a duplicate name, not to the actual file content, which may or may not be the same.

To upload folders, you need to create a Zip archive from the folder prior to the upload. This is easily done using the OS X Finder `Compress "<file>"` functionality. Windows clients (XP or later) can use the Zip archiving and extracting capability built into the Windows Explorer via the `Send To > Compressed (zipped) Folder` context menu. See also 6.8.1 “Supported upload formats”).

Note: When uploading a Zip file to the sharepoint, a dialog pops up asking if the Zip file should be extracted automatically after the upload. If you wish to prevent automatic extraction of Zip files for the whole WebShare server, please read the instructions below.

If a folder does already exist with the same name as an uploaded folder, the two folders are merged. Duplicate file names within this folder then follow the rule explained above (“dup” extension to file name).

If you wish to upload Zip archives without automatic extraction by default, you must edit the “wsupload.pl” script:

- Copy “HELIOSDIR/etc/webshare/wsupload.pl” to “HELIOSDIR/var/webshare/wsupload.pl” and change the line:

```
@unzipOpts = ("-u", "-m", $mimetype, "-o", "$fname",
"-n", "$wsmv", "-C", "$dir");
```

to

```
@unzipOpts = ("-u", "-m", "application/octet-stream",
"-o", "$fname", "-n", "$wsmv", "-C", "$dir");
```

Note: The upload mechanism supports files greater than 4 GB. In doing so, uploads will be split into smaller 2 GB chunks (default) and re-assembled on the server, to overcome browser and network web proxy limits. The chunk size can be defined by use of the **WSUploadChunkSize** preference.

Alternatively, you can upload files by dragging them into the current sharepoint file browser:

- On your workstation select the files that you wish to upload to the Webshare server and drag them into the file browser window.

You can also select several files at once, they will be uploaded sequentially.

Note: Older browsers may not support the drag & drop upload functionality. In this case the standard upload form and window are provided.

Using Internet Explorer, you must open the upload window first and then drag the file(s) into this window.

The drag & drop upload only works for file(s) – folders are not supported in HTML5. It is recommended that you create Zip archives before the upload because attributes such as color label and creation date are preserved that way.

The drag & drop functionality can be switched off completely by setting the **WSDisableHTML5Upload** preference to `TRUE`. Then, the standard upload form and window will be used (see Fig. 6.11).

Open

Open PDF documents, movies, Flash and other file types directly in the web browser. For this to work, the file must be checked in the “Select” column. Note that JavaScript must be activated in the used browser to use this feature.

Actions >

This toolbar item makes action scripts available that are stored in “var/settings/WebShare/Actions”. Corresponding icons must be named “<action>.png” and copied to “var/settings/WebShare/Brandings/<branding>/actions”. Fig. 6.13 shows an example for two action scripts, “wsl.pl” and “wssendmsg.pl”, including their corresponding icon.

The **Actions >** item in the WebShare toolbar is only available if scripts are stored in “var/settings/WebShare/Actions”!

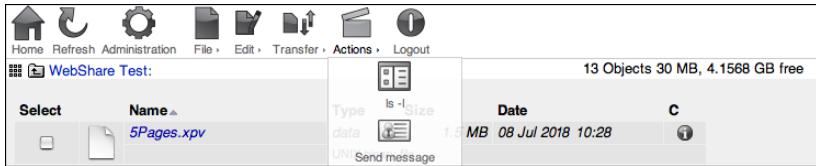


Fig. 6.13: WebShare action scripts with icon

6.3.2 Add file comments

You may add file comments, which are also available when accessing that file from EtherShare or PCShare, to any file in a WebShare sharepoint. These comments are restricted to 199 bytes.

- In the sharepoint file browser click on the **+** button pertinent to the item to add a comment.
- To read or modify an already existing comment click on the **!** button.

6.3.3 Note on file access permissions

When setting permissions on sharepoints and files, it is important to keep in mind the following file system rules that affect who can rename and delete files and folders.

File permissions

The write (“w”) permission for a file controls only the changing of the file content. This permission has no control over the renaming or deleting of that file.

Folder permissions

The write (“w”) permission for folders controls the changing of folder content, i.e. files and subfolders within that folder. The permissions set on a folder control the changing of file names and the adding or deleting of files within that folder.

Hence, if you wish to create a folder where users can read and modify files, the folder would need read/write permissions. However, if you wish to save a reference file to that folder, and do not want anyone to be able to rename or delete it, then the only way to do so is to save it into a different folder (or a subfolder), which has read-only permissions. Generally, when a WebShare user attempts to perform an action that is not allowed, either no action occurs or an explanatory error message is displayed.

Permissions: Owner, Group, Others

In addition to users who have permissions for a file or folder as described above, “root” and members of the groups “SysAdm” and “WSAdm” are also allowed to make modifications on file and folder permissions in WebShare (even if the file access permissions would not otherwise allow them to do so). Fig. 6.14 shows permissions for 2 folders and 2 files. The folder “PUBLIC” as well as the file “public.txt” are accessible by everyone. The permissions are:

`drwxrwsrwx` for the folder and `-rw-rw-rw-` for the file.

The folder “PRIVATE” as well as the file “private.txt” are only accessible by the owner (“user”), its group (“group”) and the system administrator. The permissions are:

`drwxrws-x` for the folder and `-rw-rw--` for the file.

Select	Name	Type/Ext	Size	Modification Date	C	Permission	Owner	Group
<input type="checkbox"/>	PUBLIC	dir	68	14 Jun 2019 11:07	+	drwxrwsrx	hendrik	docs
<input type="checkbox"/>	PRIVATE	dir	68	14 Jun 2019 11:07	+	drwxrws-x	user	group
<input type="checkbox"/>	private.txt	.txt	1822	14 Jun 2019 11:19	+	-rw-rw---	user	group
<input type="checkbox"/>	public.txt	.txt	834	14 Jun 2019 11:19	+	-rw-rw-rw-	hendrik	docs

Fig. 6.14: WebShare permissions

Note: Check with your server administrator for questions about permissions.

6.3.4 Logout

Clicking the `Logout` button will close all connections for that user, abort any downloads in progress and exit to the WebShare “Logged Out” page (Fig. 6.15).

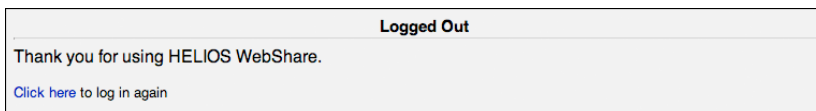


Fig. 6.15: WebShare “Logged out” page

If user closes the browser without logging out or the user has been idle for a time, i.e. no web activity has occurred, the session will automatically be closed, after the idle time period specified by the **WOSessionTimeOut** preference (see 7.6 “Preferences”).

The `Click here to enter again` link leads directly to the login window (Fig. 6.1).

6.4 Image and document previews

If the `Allow Preview` option is enabled, WebShare can generate bitmap previews when a user clicks on an image or document.

WebShare automatically detects all supported image and document types. The previews are generated by the “wspreview.pl” script which makes use of the image conversion program “wsconvert”. All previews will be generated as either JPEG or PNG files in an RGB or grayscale color space.

This script can be modified to change the default behavior. Or it can be used as a template for custom “action scripts”, e.g. to create previews with specific ICC profiles.

Images and documents

The following image and document input formats are supported:

TIFF, EPSF, DCS-1, DCS-2, Scitex-CT, JPEG, JPEG 2000, JBIG2, PICT, Photoshop, BMP, PDF, PNG, XPV, DOC, PPT, XLS, and all common RAW camera images.

WebShare can display previews of multiple-page PDF documents (also in facing pages view, with or without page break).

Note: Password-protected PDF files cannot be previewed.

QuarkXPress and InDesign (ImageServer option)

If ImageServer is installed, previews of QuarkXPress and Adobe InDesign documents (Mac and Windows) are supported. For such previews it is necessary to install the HELIOS Preview extension for QuarkXPress or InDesign. These extensions automatically save an “.xpv” file containing the document preview together upon each QuarkXPress or InDesign document save. A WebShare user can click on this “.xpv” file to view the document previews of each page.

Office documents

Previews of Office documents in WebShare are possible. Please read the **Custom preview types** section.

Generated previews

WebShare generates PNG previews for the following formats:

- PDF
- QuarkXPress & InDesign documents (“.xpv”)
- All images containing a clipping path
- 1 bit images (black/white)

WebShare generates JPEG previews for the following formats:

- All grayscale and color images without a clipping path

All previews and proofs, once generated, will be cached to allow the reuse of existing rendered previews by other users.

It is possible to customize the preview generation by using different ImageServer parameters in the “wspreview.pl” script, e.g. to specify a different ICC profile for the RGB color space that is used for the previews.

The following resolutions are supported by default:

- Zoom 1: 256 pixel (default image width after clicking on image)
- Zoom 2: 512 pixel
- Zoom 3: 768 pixel
- Zoom 4: 1024 pixel


Additional preview resolutions can be specified as pixel or dpi values on the “Server Preferences” administration page. The customizable resolutions are selectable in the pop-up menu. The preview resolutions should be limited to avoid very large preview images which may take very long to download and display within the browser. Zoom 1 to Zoom 4 are defined in the “Branding Editor > *Branding Name* > Preview Resolutions 1-4” preference.

Note: If JavaScript is not enabled, clicking the Go button will start generating the preview specified in the pop-up menu.

6.4.1 Previewing images and single document pages

WebShare allows previewing images and supported document formats (see 6.4 “Image and document previews”). If this feature is enabled for a sharepoint, then file names will appear as links.

- To view an image or document, click on the file name or select one or more files and click the File > Preview toolbar button.

If multiple items have been marked for preview in the file browser, the first preview is displayed, other(s) can be selected from a pop-up menu or via the “next” and “previous” arrow icons (Fig. 6.16). A checkbox adjacent to the pop-up menu allows unselecting images in the file browser (go back with .

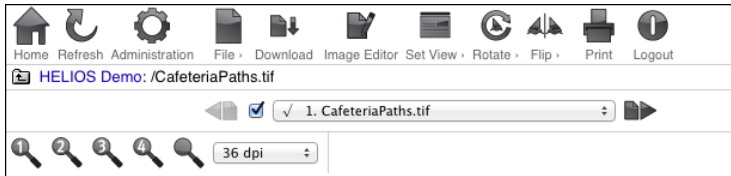


Fig. 6.16: Select preview from pop-up menu

Previews can be scaled in resolution and dimensions via the “zoom icons” or the pop-up menu adjacent to them (Fig. 6.16). The dimensions, resolutions (and percentage values), which are also available in the `Set View >` button in the toolbar, can be specified in the `Preview Resolutions (pixel or dpi)` field of the WebShare “Server Preferences” page. The “zoom icons” have fixed resolutions which can be defined per branding, in the Branding Editor, by use of the “Zoom 1-4” preference (see 4.7.1 “Create and configure brandings”). The default values are 256, 512, 768, and 1024 pixels. The zoom icon on the far right has WebShare display the preview in full-screen mode. If you have specified monitor width values in the `Monitor Size Information` section in “My User Preferences”, the entry 100% is available in the `Set View > Zoom` menu or in the resolution pop-up menu, to display the preview images in their original size.

The `Rotate >` and `Flip >` toolbar icons allow transforming the preview according to the action selected in the corresponding submenu. The selected view settings (zoom, rotate, flip, info) are maintained for subsequent previews.

`Set View > Show/Hide Image Info` allows controlling whether basic image information is displayed along with each image.

6.4.2 Image Editor

Important: To make use of Image Editor it is required that ImageServer be installed. Also, Image Editor requires download permissions on the sharepoint, otherwise the Image Editor icon in the menu bar will appear grayed-out.

The “Image Editor” function allows the user to apply simple changes on an image document. Images can be rotated, flipped vertically and horizontally, and cropped. In addition, the edited images can be downloaded from the WebShare server in five presets, which can be selected from the `Output` drop-down list (see Fig. 6.17).

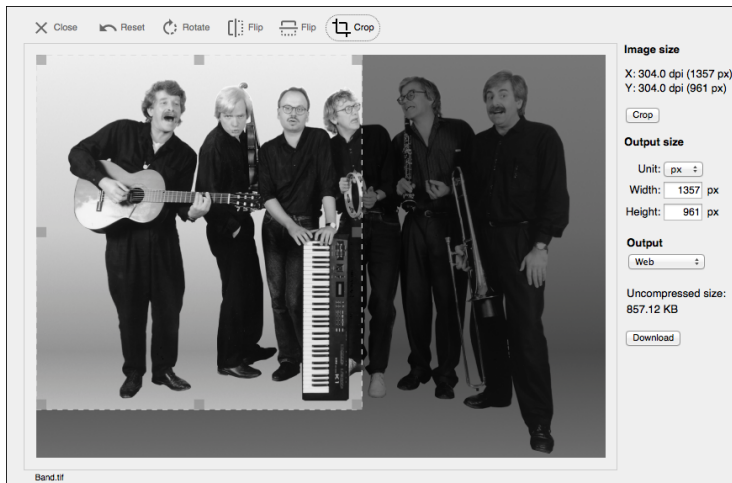


Fig. 6.17: Cropping an image using the “Image Editor” function

○ **Web**

This setting is useful for publishing the edited image on the web.

- Format: JPEG/PNGf
- Color: RGB
- Compression: JPEG/PNG
- Resolution: 144 dpi
- Profile: sRGB_IEC61966-2-1_noBPC.icc

○ **Office**

This setting is useful for using the edited image in an MS Office application, e.g. Word.

- Format: JPEG/PNGf
- Color: RGB
- Compression: JPEG/PNG
- Resolution: 144 dpi
- Profile: sRGB_IEC61966-2-1_noBPC.icc (if input file = CMYK => no profiling)

○ **Prepress**

This setting is useful for using the edited image in a prepress environment. It will maintain its high resolution and is converted to the CMYK color space, for proper printing.

- Format: TIFF
- Color: CMYK
- Compression: compress
- Resolution: 305 dpi
- Profile: ISO-coated_v2_eci.icc (if input file \neq CMYK)

○ **PDF**

This setting embeds the image in a PDF document, for easy sharing and viewing. Lossless JPEG2000 compression reduces the file size considerably.

- Format: PDF
- Color: RGB
- Compression: JPEG2000

- Resolution: 144 dpi
- Profile: sRGB_IEC61966-2-1_noBPC.icc

○ **PDF Hi-Res**

This setting is similar to the standard PDF preset with the difference that the high resolution of the original image is maintained. Lossless JPEG2000 compression reduces the file size considerably.

- Format: PDF
- Color: RGB
- Compression: JPEG2000
- Resolution: 305 dpi
- Profile: sRGB_IEC61966-2-1_noBPC.icc

Note: If an image is downloaded with its original dimensions (width, height), WebShare sets its resolution to the value defined in the used preset, e.g. *144 dpi* (“Web” and “Office”). Width and height of the output image are adjusted accordingly, and differ from the original dimensions.

However, if width and height of the image are modified, then these values are used in the output image, but the resolution is changed accordingly. For output sizes specified in *cm* or *in* the resolution defined in the used preset is delivered, and the dimensions are adjusted accordingly.

Edit an image

Here is a short example on how to crop an image and then save it using the “Office” preset:

- From within the preview mode, click on the `Image Editor` button in the toolbar to open the image editor window.
- Click on the `Crop` tool to activate the crop mode (see Fig. 6.17).
- Drag the cropping tool rectangle over the area that should remain after cropping.
- Click on the `Crop` button to apply your changes to the image.

- Specify the output size and select “Office” from the `Output` drop-down list.
- Click on the `Download` button.

Customize Image Editor output settings (output drop-down list)

The Image Editor output pop-up list offers five standard output settings. To modify these settings, or set up your own presets, you need to create – if not already available – the file “additional.js” in the branding folder “var/settings/WebShare/Brandings/<branding name>”. It will automatically be included in every WebShare server response for the corresponding branding.

As a starting point you can use is the example file “additional_samples.js”. It is copied to “var/settings/WebShare/Brandings/default” during the WebShare installation. It contains information and examples about using JavaScript to customize the behavior and adding custom functionalities to a WebShare branding:

- Copy “additional_samples.js” to the desired branding subfolder and edit it, or create a new UTF-8 encoded text file and add custom JavaScript code to this file. In any way, save it as or rename it to “additional.js”.
- On the WebShare “Branding Editor” page click on the “`Import Brandings from WebShare File Server.`” link.

Example:

Delete all entries from the Image Editor output drop-down list and add two entries named “Documentation” and “HiRes”:

```
var ieOutput = document.getElementById("ie_output");
if (ieOutput) {
    for(var i = ieOutput.options.length - 1; i >= 0 ; i--) {
        ieOutput.options.remove(i); // delete existing entries
    }
    // create a new entry
    var option1 = document.createElement("option");
    if (document._locale == "de")
        option1.text = "Für Doku"; // German localization (consider
        localization for supported locales DE, ES, JA)
    else
```

```

        option1.text = "Documentation"; // default language (English)
option1.value = "id=docu; res=72; colorspace=RGB; format=PNGf;
icc='sRGB_IEC61966-2-1_noBPC.icc';
ieOutput.options.add(option1); // add new entry

// create a second one
var option2 = document.createElement("option");
if (document._locale == "de")
    option2.text = "Hohe Auflösung"; // German localization
    (consider localization for supported locales DE, ES, JA)
else
    option2.text = "HiRes"; // default language (English)
option2.value = "id=hires; res=305; compress=compress;
colorspace=CMYK; format=TIFF; icc='ISOcoated_v2_eci.icc';
ieOutput.options.add(option2); // add new entry
}

```

Editing images in multi-page documents

The **Rows** and **Cols** buttons in the toolbar allow displaying several pages at the same time (see 6.4.5 “Previews of multiple-page documents”). The user can select one of the pages to edit it in the “Image Editor”.

6.4.3 “Color Info”

Important: For the “Color Info” feature, HELIOS PrintPreview must be installed.

Color info for PDF documents is only available in proof mode and only if a simulation profile has been selected.

Set View > Color Info is similar to the Photoshop color info and shows the individual primary color and spot color values used in the selected area (Fig. 6.18).

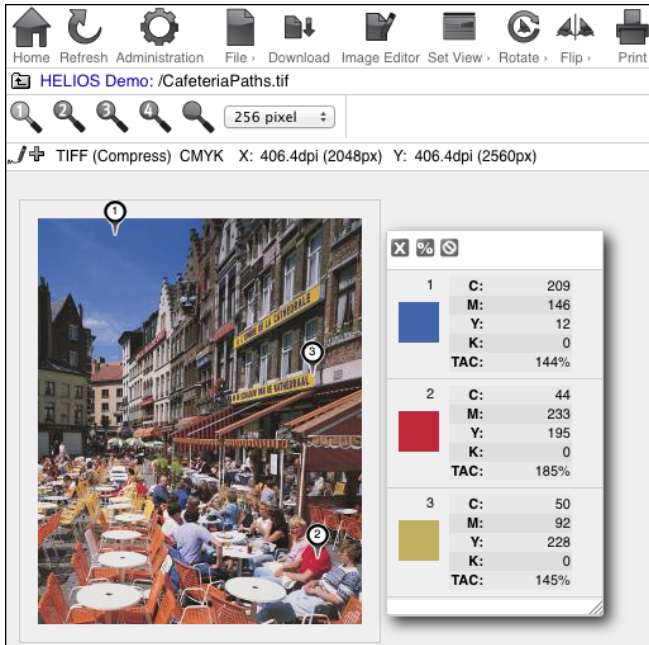



Fig. 6.18: The Color Info dialog

- To obtain color information, open the color info window by selecting `Set View > Color Info` and click on the preview or proof image.

Note: Color information for PDF documents is only available in proof mode and with a selected simulation profile.

The color values can be displayed in bit or percent values. The `%` icon in the title bar can be used to toggle between these display modes. When retrieving color information of CMYK images, the TAC (*Total Area Coverage*) is also displayed in addition to the process color values.

➤ To clear the list of color value entries, click the  icon in the title bar.

Every click on the preview or proof image will leave a numbered marker which belongs to a list entry of the same number. If you hover over a list entry the corresponding marker will be animated, a click on a list entry scrolls the corresponding marker into view. A click on an image marker highlights the corresponding list entry and scrolls it into view. The “Color Info” dialog can be dragged by clicking on the title bar and resized to the required size.

Note: If color information for high-resolution image are retrieved while the preview resolution is relatively low, it can happen that the displayed results do not match the actual values. In this case the interpolation of the position where you have clicked to is to blame.

6.4.4 “Annotations”


Important: For the “Annotations” feature, HELIOS PrintPreview must be installed!

JavaScript must be activated in your web browser to enable the annotations feature!

The annotations feature is *not* supported by Internet Explorer 6. Internet Explorer 7 and newer however do support this feature.

In order to make the annotations feature available for the current sharepoint, the `Allow Annotations` checkbox must be activated (see 4.5 “Sharepoint Administration”).

`Set View > Annotations` opens a dialog window, which allows attaching annotations to all file formats that can be previewed with WebShare (see 6.4 “Image and document previews”). It tracks document versions and allows signing off ready-to-go documents (Fig. 6.20).


A discussion is opened by clicking on the  icon in the left upper corner of the annotations dialog, and marking a point or a rectangle area in the document, which starts a new reviewing thread. A rectangle area marker allows selecting



the marker color from a color picker and its opacity. From the pop-up menu `Status`, each user can specify within the annotation thread, if they agree or reject the issue, or leave everything as is. The next user can reply to an annotation by clicking the `Reply` button underneath the entry to which they wish to answer and set a new thread discussion status. If a discussion thread already exists, the overall status is displayed adjacent to the file information in the WebShare preview window (see Fig. 6.20 below).

After *all* threads of a document are answered in an accepted state, the document turns into final. Multiple document versions and multiple threads are supported.

An already existing discussion can also be opened by clicking the overall status icon or by clicking on the desired “<file name>.annotation” entry in the WebShare file browser.

Annotations and their replies can be edited or deleted later. However, this is only possible with your own annotations and answers, provided they are still unanswered. Annotation topics can be sorted by date, in multi-page documents additionally by page (each topic corresponds to a point or rectangular marker).

The metadata dialog () shows the file name, and allows specifying a project name and a due date (see Fig. 6.20). The project name is displayed in the annotation title.

The  /  buttons allow expanding/collapsing the whole annotations thread. If the thread is collapsed, date and time of the last contribution are displayed (compare Fig. 6.19 with Fig. 6.20).

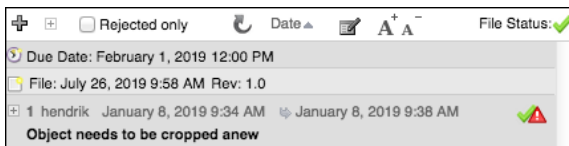


Fig. 6.19: Date and time of last contribution

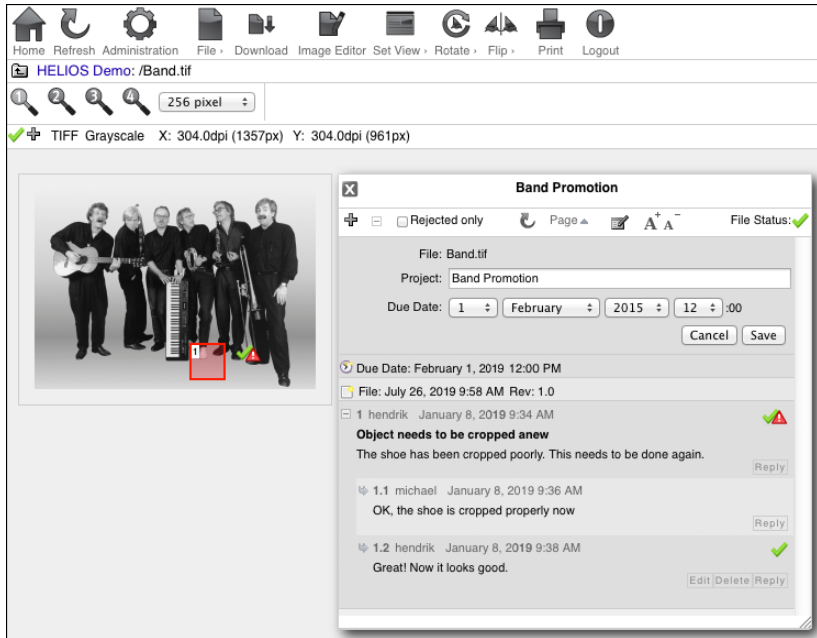


Fig. 6.20: Annotations to an image file

The whole discussion is stored in a look-aside XML file, which stays next to the document. The (**AnnotationPrefix**) preference allows hiding the XML file or storing it in a directory. The XML format allows parsing the annotation records or automatically generating annotation files.

This also addresses all requirements to collaborate within a remote proofing workflow. Especially the multiple-version document support allows keeping the entire history and differentiate between versions. The annotation capability works for the WebShare document preview and proofing window.












Icon	Description
	Add an annotation
	Expand all/Collapse all annotations
	Edit the annotation metadata, e.g. project name and due date
	File status: Accepted, the document is final
	File status: Rejected, there are conflicts
	Revision status: File has changed since last annotation
	Annotations for a document exist but no status was set
	Document was viewed in proof mode with ICC profile selected when annotation was saved
	Increase or decrease the font size
	Refresh annotations view and send pending e-mail notifications
<input type="checkbox"/> Rejected only	Filter to display rejected entries only

Table 6.2: Icons used in annotation dialog

WebShare annotations can be printed out using the WebShare print function () , see 6.4.7 “Preview/proof print settings”. The first page will contain the image with its marks, the following pages will show the comments.

6.4.5 Previews of multiple-page documents

If you open a multiple-page document, the toolbar is extended to offer more functions (Fig. 6.21):



Fig. 6.21: WebShare multiple-page preview toolbar

You may navigate through the document by entering the desired page number and pressing the ENTER key or the “Refresh” button of the toolbar, or you can flip the pages forward and backward.

In addition, you can add or remove rows and columns for previewing multiple-page documents. This can also be done in the `Set View > Rows/Cols >` toolbar menu. Presets are available in the `View Presets >` submenu: 2x2, 2x4, and 4x4 rows/columns.

Note: The maximum number of concurrently displayed preview images is 300.

`Set View > Options >` makes two more preview options for multiple pages available:

Facing Pages

The pages of a document face each other, with the even numbered pages being always on the left and odd numbered pages on the right (Fig. 6.22).

Note: Multiple-page documents are considered as books if `Facing Pages` is selected. Therefore the first page of a document is always displayed single.

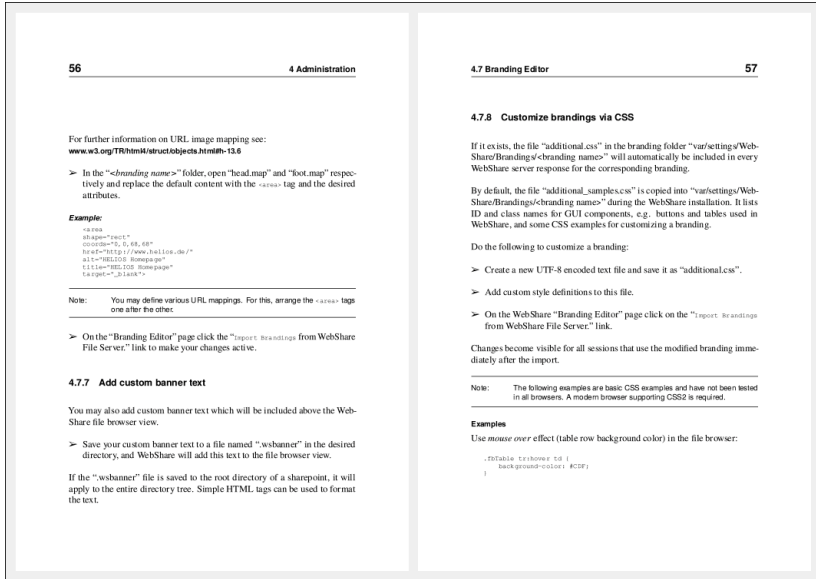


Fig. 6.22: Multiple facing pages

Page Breaks

The gap between facing pages is removed if the Page Breaks option is *unselected* (compare Fig. 6.22 and Fig. 6.23).

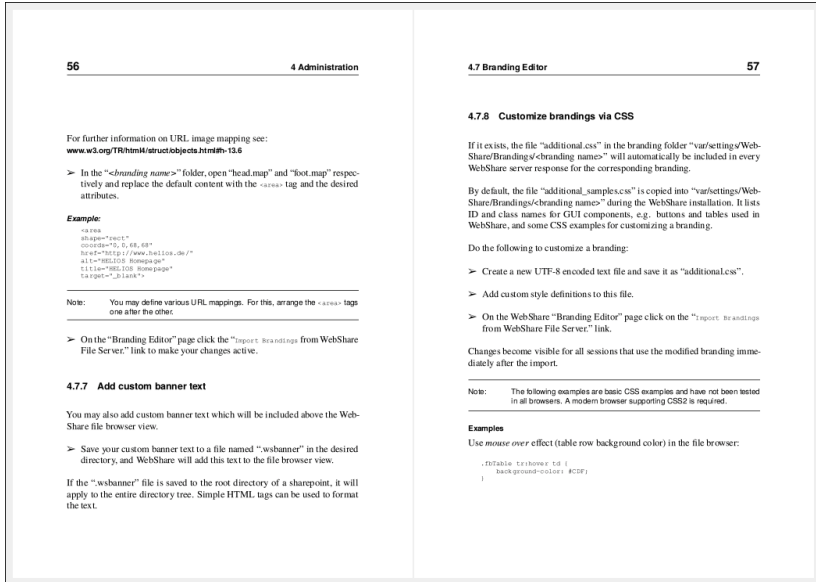


Fig. 6.23: Multiple facing pages without page break

6.4.6 Banner and trailer files per document

To display file-related information in the file preview, WebShare searches the current directory for files with the same file name and a ".banner" or ".trailer" suffix, and displays the content of these files in the file preview. For example, the files "Cafeteria.tif.banner" and "Cafeteria.tif.trailer" will be displayed above/below the file preview of the file "Cafeteria.tif". HTML content is allowed for these files.

6.4.7 Preview/proof print settings

A click on the `Print` toolbar icon allows specifying print settings prior to using the standard OS print dialog, when printing a preview or proof image (see Fig. 6.24).

The `Paper Size` pop-up menu allows choosing a pre-defined paper format from the list, or `Custom...` which opens the `Extended Options` dialog. Here you can specify custom values for the page dimension, and in addition define a scaling factor. The values that are specified are used for scaling and positioning only and it is important that they match those selected in the browser dialogs “Print” and “Page Setup”, respectively. The “Paper-Formats.txt” document, which is located in the “WebShare Public” sharepoint (“Proof-Templates” directory), contains all those paper formats that become available in the `Paper Size` pop-up menu.

Note: If you check the `Scale Images To Fit Page` option, the chosen scaling factor may be overridden.

The `Resolution` pop-up menu allows selecting the resolution for printing the document:

```
Draft (150 dpi)
Good (240 dpi)
Excellent (300 dpi)
Super Fine (400 dpi)
```

Note: By default, or if `PrintPreview` is not installed and licensed on the server, the resolution of the preview image is 150 dpi.

If the `Print Annotations` (`PrintPreview` required!) and `Print Images` options are checked, the first page will contain the image, the following pages will contain the annotations.

In proof mode, an additional checkbox, `Print Image Info`, becomes available. If this option is checked, the image information is included in the printout.

Preview/proof print settings for multiple-page documents

When printing multiple-page documents, the “Print Settings” dialog offers an additional section (Fig. 6.25) which allows specifying the printing range. `Current view` prints the page(s) displayed in the browser, or a range of pages when using the `From` and `To` fields. If you wish to print only those pages that contain images with annotations, use the `Images With Annotations Only` option.

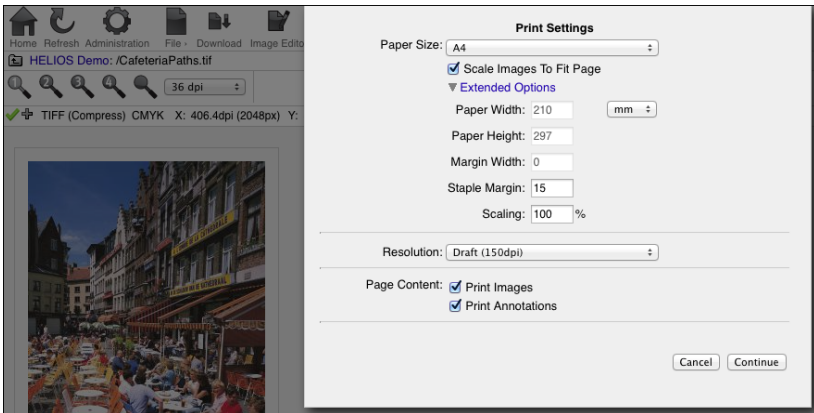


Fig. 6.24: WebShare preview/print dialog

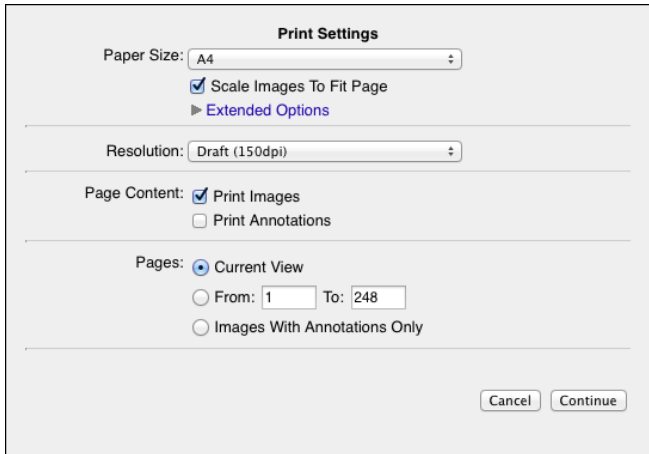


Fig. 6.25: WebShare preview/proof print dialog for multiple-page documents

For the print output of the preview, workstation-based color management (sRGB v4 ICC) is applied.

6.5 Remote Proofing

Together with HELIOS PrintPreview, WebShare allows remote soft proofs on the monitor and color-matched proof prints from the web browser.

The remote proofing feature is described in detail in the HELIOS PrintPreview manual.

6.6 WebShare Quickshares

A “Quickshare” is a short URL that allows sharing a group of files on the WebShare server to remote users, without the need to set them up as users or configure a new sharepoint. Quickshare links allow users to download, upload and preview files via a simplified WebShare user interface. In addition, Quickshare URLs can be specified with a duration date, after which they expire.

To be able to use Quickshares, make sure that the server option `Allow Quickshares` (see 4.1 “Server Preferences”), and the sharepoint option `Allow Quickshares` (see 4.5 “Sharepoint Administration”) are enabled. See also 4.2 “Quickshare Administration” which describes how to manage existing Quickshares, and `Quickshare User` (see 4.3 “User Administration”), which discusses the “Quickshare User” settings.

6.6.1 Create Quickshares

- Select a file in the sharepoint file browser and choose `Edit > Quickshare` from the toolbar, or alternatively, choose `Quickshare` from the contextual file menu (see **Contextual file menu** in 6.3 “Work in a sharepoint”) of the file for that you wish to create a Quickshare.
- Choose `Create new user` from the `User` pop-up menu and enter a *new* user name in the `New User` field. Then specify a password (optional) and a valid e-mail address in the corresponding fields.

If you have already created another Quickshare for a certain user, and you wish to assign this new Quickshare to the same user, select them from the pop-up menu instead.
- Specify what actions the recipient of the Quickshare should be allowed to take via the `Preview`, `Download`, and `Upload` checkboxes.

- From the `Expiry` pop-up menu choose an expiry date, or specify a custom date. In addition, you may enter a comment which is provided to the recipient of the Quickshare.
- If you wish to be notified as soon as the recipient opens the Quickshare check the `E-Mail on Access` checkbox.
- Click on `Save` when you have completed all entries.

The user who is assigned a Quickshare can be provided a direct link to the Quickshare (`Send E-Mail to <Quickshare user>`).

Delete a Quickshare user

- In the sharepoint file browser select an arbitrary file and choose `Edit > Quickshare` from the toolbar, or alternatively, choose `Quickshare` from the contextual file menu (see **Contextual file menu** in 6.3 “Work in a sharepoint”) of any file.
- In the `User` pop-up menu choose the user that you wish to delete. Then click on the `Delete` button and confirm the deletion.

6.6.2 Manage your own Quickshares

`Administration > Quickshare Administration` allows a user to edit existing Quickshares, or delete them. A description of this window can be found in 4.2 “Quickshare Administration”. Users who are not WebShare administrators can manage only the Quickshares that they have created, whereas WebShare administrators can see all Quickshares, including information about the creator of each Quickshare.

6.6.3 Upload files to a Quickshare

Files uploaded to a Quickshare are incorporated in a folder named “Quickshare Upload-<Quickshare user name>-<number of Quickshare>”. This folder is always stored in the Quickshare root directory.

6.7 My User Preferences

In `Administration > My User Preferences` personal user settings (Fig. 6.26) can be specified. The dialog allows the user to specify individual settings for downloading files, which may well override the settings specified by the administrator on the “User Administration” page.

Settings for User <user name>

With the `Preferred View` pop-up menu, the user can define their preferred initial file browser view. It offers: `Default`, `Smart Extended`, and `Small`. The additional option `Gallery` is only available if the gallery view is activated.

The `Download Encoding` pop-up menu offers `MacRoman`, `PC850`, `ISO8859-1`, `UTF8`, `MacIcelandic`, `EUC-KR`, and `SJIS` encoding methods. In addition, `OS Default` uses the client OS default encoding, which was set by the administrator.

With the `Zip Streaming Format` checkbox activated, the file download uses *Zip streaming* (instead of a standard Zip file download), which allows file compression *on-the-fly*, without creating any temporary files.

- After changing your user preferences click on the `Save User Preferences` button. Otherwise your changes will get lost.

Home Refresh Administration Logout

My User Preferences

Settings for User "demouser"

Preferred View:

Download Encoding:

Zip Streaming Format:

E-Mail Address: henk@helios.de

Change WebShare Password

Old Password:

New Password:

(Crypted RSA 1024 bit)

Proof Setup

Default Monitor Profile:

Server color management: matched against selected profile, profile is omitted

Default Printer Profile:

Workstation color management: matched with server default profile, profile is included

Default Simulation Profile:

▼ **Monitor Size Information**

Width (pixel):

Screen Width:

▼ **Monitor Profile Administration**

Select	Name	Modification Date
<input type="checkbox"/>	Apple Performa Display	01 Dec 2018 10:38

▶ **Printer Profile Administration**

▼ **Simulation Profile Administration**

Select	Name	Modification Date
<input type="checkbox"/>	SC_paper_eci.icc	24 May 2015 15:14

Fig. 6.26: WebShare "My User Preferences" page

Save Default User Settings

Note: This section is only available to users with administrative rights.

With the `Save Default Settings` button the admin user can save their personal settings as default settings for all other users. The settings are stored in “HELIOSDIR/var/run/WebShare_User_Settings/WSdefaults.settings”. The default settings are overridden by personal user settings.

Any custom JavaScript properties (see 8.2.1 “WSProperties”) and data entered in the “Monitor Size Information” section (properties starting with `Default.screen.< ... >`) will not be saved in the default user settings.

Change WebShare Password

In addition, the “Change WebShare Password” section allows WebShare users to change their WebShare password on their own, without having administrative rights on the WebShare File Server. This is another means of security for *Host Users* who may not want to use their host user password over the internet. For example, a remote login to WebShare from an internet café bears the risk of a spied host user password (e.g. keystroke logging spyware can capture a password as it is typed in, before the password is encrypted for transmission). If someone uses their host user name but a password that is only used with WebShare, the worst-case scenario would be a spied WebShare login, with the host login not being affected. For more information on content security see also 10.1.10 “No content security”. Of course, *Virtual Users* can also change their password on their own in this configuration window.

Note: Users which were assigned the “Cannot change Password” flag by the administrator cannot change their WebShare password on their own (see **Create users** in 4.3 “User Administration”).

- Enter the old (existing) and the new password in the respective fields. To use the existing host user password again, *Host Users* leave the `New Password` field blank. For *Virtual Users*, any attempt to leave the `New Password` field

blank will yield an error message. In this case the “original” WebShare password has to be entered again.

Proof Setup

If `Allow ICC Profiles per User` is activated on the `Server Preferences` page (4.1 “Server Preferences”) the user can choose their default profiles by use of the `Default Monitor Profile`, `Default Printer Profile`, and `Default Simulation Profile` pop-up menus. The chosen profiles will automatically be selected in the `Monitor ICC Profile` and `Printer ICC Profile` pop-up menus in the WebShare proof window. Selecting a profile will switch the proofing mode from “Workstation color management” (profile is included in image, default behavior) to “Server color management” (profile is omitted). If no profiles are available on the server, the buttons `Add Monitor Profile`, `Add Printer Profile`, and `Add Simulation Profile` open an upload dialog.

Note: If a simulation profile has been added via the `Add Simulation Profile` button, all default simulation profiles defined in the “Server Preferences” page will disappear from the `Default Simulation Profile` pop-up menu.

With the `Monitor Size Information` link the visibility of the preferences `Width (pixel)` and `Screen Width` can be switched. With these properties the user may enter their monitor width in pixels in the `Width (pixel)` field and the width of the visible screen size in a selectable unit (mm, cm or inch) in the `Screen Width` field. If both preferences are set, the entry `100%` becomes available in the `Set View > Zoom` menu of the file preview and proofing page to display images in its original size. If JavaScript is activated, the `Detect` button next to the `Width (pixel)` field can be used to automatically detect the pixel width.

WebShare will remember if a zoom level of `100%` has been selected for the proof component, and will add this setting to the user settings file. When the component is opened again, the proof will be displayed at 100%, even with a new login. If another zoom level is selected, the setting is deleted from the user settings file.

If any global or user ICC profiles are available on the server, the user can have these profiles displayed in the `Monitor Profile Administration`, `Printer Profile Administration`, and `Simulation Profile Administration` sections. Profiles added by the user can be deleted by selecting the profiles and clicking the `Remove Selection` button. The `Add Profile` button opens a dialog to upload an ICC profile. Global profiles are displayed *grayed-out* and cannot be administered by the user. The profiles are stored in the “.Proof-Profiles/<username>/Monitor”, “.Proof-Profiles/<username>/Printer”, and “.Proof-Profiles/<username>/Simulation” folders of the root directory of the “WebShare Public” sharepoint.

Note: `Allow Preview` has to be enabled for the “WebShare Public” sharepoint. The server preference `Allow ICC Profiles per User` has to be enabled and the “WebShare Public” sharepoint must be published for this feature.

6.8 WebShare file format support

6.8.1 Supported upload formats

- Uncompressed single file
- Windows XP (or newer) Explorer Zip files
- WinZip archives (8.1 or newer)
- MacBinary encoded file
- OS X 10.3 (or newer) Finder Zip archives
- Mac OS 8/9 DropZip 7.0.3 archives (MacBinary)
- OS X DropZip 8.0.2 files (MacBinary)

We recommend to use the Zip format for uploading because they

- ... have a high compression ratio
- ... can contain multiple files/folders

- ... support Mac OS Resource/Finder information (MacBinary)
- ... preserve the file creation date
- ... preserve special characters in file names

6.8.2 Supported download formats

- Zip-compressed archives for UNIX and Windows clients
- Zip Streaming format supported by Windows XP (or newer), and by Mac, using Mac Finder Zip (OS X 10.3 or newer)

6.9 Supported browsers

WebShare uses standard HTML web pages. Special browser plug-ins and Java are not needed. JavaScript is used to ease access to some features and to improve the overall appearance. However, WebShare generally works well without JavaScript being activated in the browser. WebShare has successfully been tested with many different browsers on Windows, Mac OS 9, OS X and UNIX platforms. For power users, this chapter provides information about which browsers have intensively been tested by HELIOS, and some hints about possible problems.

- Safari 3.0 and newer
- Firefox 3.0 and newer
- Internet Explorer 6 and newer
- Google Chrome 5.0 and newer
- For mobile devices, see 9 “HELIOS Document Hub”

These above listed browsers have received more intensive testing and are considered to work perfectly with WebShare. Again, many other browsers will just work fine with WebShare but have only received limited testing.

Please note that iOS does not support downloads.

Automatic MacBinary upload support

All current browsers skip MacBinary data so that the document resource (e.g. preview picture, icon, document type) gets lost during the upload.

Solution:

Instead of uploading just files, generate OS X Finder Zip archives. Uploading the compressed Zip files will work with any browser.

Continuing browsing while uploading files

Some browsers do not accept additional requests while they are uploading files (refer to your browser documentation). A new browser window or using a different browser application allows logging in a second time and continuing with other tasks or monitoring the loading files. The disadvantage of the second login is that it will require one additional user session on the WebShare File Server.

Safari allows continuing while the upload is ongoing.

Saving a password in your browser/keychain

As WebShare crypts all passwords with a random number for every login, re-using the same old password does not work for a second time. Browsers may cache the user name and passwords and try to re-use it a second time, which fails with the WebShare login. HELIOS considers this a security feature of WebShare.

In case JavaScript is turned off the password is sent unchanged (in clear text) to the server, and the keychain/browser feature remembering this clear text passwords works again. We recommend to keep JavaScript active to allow encrypted passwords for the WebShare Server login.

Downloading progress bar does not match downloaded file size

When downloading files, the WebShare Zip streaming technology compresses files always *on-the-fly* during the download. The browser progress bar shows the uncompressed original size. However, the download size will differ due to the zipstream compression and additional changes on the server before the download is completed. The very last file in every download is called “DownloadLog.txt” which includes a list of all downloaded files and possible errors (file was not accessible anymore, no permission, etc.). If this file is included after unpacking the “download.zip” archive you can assume a complete download.

Do not use the back/forward buttons of your browser

WebShare keeps some state about the current directory, selected files, etc. Using the back button, the client will request a page and may use the selection of the previous page instead of the current one. This can lead to unpleasant results, e.g. if the selection was “delete files”. Only the “Home” window allows to open a separate window for each sharepoint. Do not use the back/forward buttons or the “Open Link in new Window” option of your browser. The central “Home” menu or selectable URLs in the file browser allow you to go back to different locations.

7 WebShare Web Server

The WebShare Web Server (“webshare.woa”) is a Java program running on a server with an internet connection. It can be installed on the same machine where the WebShare File Server is installed, in which case it is called a “single server solution”. To increase the level of file system security, the WebShare Web Server should be installed on a separate server, in a “two-tier server solution”.

Ideally no other applications or services would be running on the WebShare Web Server. This allows the blocking of all ports and services (by software and/or hardware firewalls), except for those required by WebShare.

Due to the fact that no data files are stored or cached on the WebShare Web Server, a high level of WebShare File Server security is ensured. The WebShare Web Server uses one dedicated TCP/IP port for all web clients, by default 2009.

During the installation of HELIOS WebShare the packed file “websharewoa.tar” is installed in the directory “HELIOSDIR/etc/webshare”. The “start-helios” command then extracts the file in the directory “HELIOSDIR/var/run” to the “webshare.woa” package.

7.1 WebShare license information

The WebShare product includes two server components. The WebShare File Server which is licensed on a given HELIOS machine ID (mach ID) and a WebShare Web Server which may run on a separate server machine. The

WebShare Web Server belongs to the WebShare server product and will not require a separate WebShare activation key.

The complete HELIOS software license terms must be accepted during the installation and can be found on the product CD.

7.2 WebShare Web Server files

The “HELIOSDIR/var/run/webshare.woa/Contents/Resources/” folder contains the following files:

Accounting.wo/

Accounting HTML page component

AccountingDetails.wo/

HTML page component for detailed accounting information

AdmPrefs.wo/

Preferences administration HTML page component

AdmShares.wo/

Sharepoint administration HTML page component

AdmUsers.wo/

User administration HTML page component

Admin.wo/

Main administration HTML page component

FileBrowser.wo/

HTML component for browsing files and directories

FilePreview.wo/

HTML component for document and image previews

ForgotPassword.wo/

Template HTML component for forgotten passwords

Goodbye.wo/

Logout HTML page component

Login.wo/

Login HTML page component

Main.wo/

Welcome and select server page component

PagePreview.wo/

HTML component for image proofs

RegisterNewUser.wo/

Template HTML component for registering new users

Sharepoints.wo/

Sharepoint listing HTML page component

Upload.wo/

HTML component for uploading files

UserPrefs.wo/

User preferences HTML page component

WSBrandingEditor.wo/

HTML Branding Editor component

WSCSSComponent.wo/

System internal component

WSExceptionPage.wo/

System internal component

WSFileAnnotationsContent.wo/

System internal component

WSFileAnnotationsEntryContent.wo/

System internal component

WSFileAnnotationsTemplate.wo/

Template for annotations dialog

WSFileListingMenu.wo/

System internal component

WSOpenFile.wo/

Template for open file page

WSToolbar.wo/

HTML toolbar component

WSToolbarButton.wo/

System internal component

WSToolbarLink.wo/

System internal component

WSUploadForm.wo/

System internal component

WSUploadReport.wo/

System internal component

WSUploadStatus.wo/

System internal component

WebShareStats.wo/

Server statistics HTML page component

ZipDownload.wo/

System internal component

Each “*.wo” directory contains the “*.html”, “*.wod” and “*.woo” files for the corresponding web page.

The script “sbin/start-websharewoa” starts the WebShare Web Server daemon. Usually, it is started by the “srvutil start websharewoa” command during “start-helios”. In case of startup problems, it can be started manually to monitor the error messages in a terminal window via:

```
# cd /usr/local/helios
# sbin/start-websharewoa
```

Additional logging is reported to the WebObjects log files. They are located in “HELIOSDIR/var/adm/” and are called “websharewoa.log”, with the appendices “.0” (*yesterday*), to “.6” (*seven days ago*). All internal WebObjects messages are reported to “websharewoa.log”. All HELIOS generated WebShare Web Server messages are reported to the system messages file.

7.3 Customization/Localization

WebShare includes user selectable localized language support for its user interface. This chapter describes how to customize an existing language version.

Note: This section is about customizing the “webshare.woa” package. If no customizing is done, then this section can be ignored.

- To customize the WebShare Web Server, first copy the “webshare.woa” package from “HELIOSDIR/var/run” to “HELIOSDIR/var/webshare”.

All customization must be done in “var/webshare”. This is because whenever WebShare is started it looks for “webshare.woa” in “var/webshare”. Only if it cannot be retrieved from there, is it taken from “var/run”. The idea is that “webshare.woa” is always replaced in “var/run” in case of software updates. Being in “var/webshare”, localizations and other adjustments are preserved.

Note: However, for new WebShare product versions or updates that incorporate new features, you must copy the “webshare.woa” package anew from “var/run” to “var/webshare”, overwriting the older package, and apply the customization/localization again. Otherwise it might be incompatible with the used WebShare File Server or new features might not be available.

7.3.1 Customizing “*.html” files

Customize all “*.html” files, using UTF-8 characters. Before changes in “*.html” files become valid, the “websharewoa” service must be stopped and restarted.

7.3.2 Customizing “*.wod” files

Customize all “*.wod” files, using UTF-8 strings. You may customize the strings with any UTF-8 compatible text editor. Before changes in “*.wod” files become valid, the “websharewoa” service must be stopped and restarted.

7.3.3 Customizing action scripts

Custom action scripts are customized by putting `#Title=UTFname` into the script within the first 5 lines.

Likewise, the `#NameField=` comment in any script can be edited. The next time you log in and select a script from the WebShare “Actions” toolbar item, a field becomes available, allowing you to submit values to the script.

Refer to 8.4 “WebShare scripts” for details on creating or customizing WebShare custom scripts and action scripts.

7.3.4 Adding additional language localizations

WebShare includes support for English, German, Japanese, Spanish, and French. Additional language localizations can only be done directly by HELIOS. Please contact your HELIOS partner for such requests.

Note: If customizations should also be valid in localized resources, then the “<language>.proj” folders must also be customized.

7.4 HTTP/SSL support

7.4.1 Introduction

This section outlines how to configure your SSL setup. We will describe how to use the HELIOS “wskeytool” utility to accomplish this task.

What does SSL mean?

SSL (*Secure Sockets Layer*) is a protocol designed by *Netscape Communications Corporation* to provide encrypted communications on the internet. SSL is layered beneath application protocols such as HTTP, SMTP, FTP, Telnet, Gopher, and NNTP and above the connection protocol TCP/IP. It is used by the HTTPS access method. SSL works by using a secret key to encrypt data

that is transferred. Modern browsers support SSL, and many websites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http:*.

7.4.2 Background

An SSL-enabled server usually uses a secured file or database called keystore to store the keys and certificates for the server. These security credentials are used to prove to clients that the server is legitimately operating on behalf of a particular domain. If your server will only need to act as one domain, you only need one key entry and certificate in the keystore. Keys are stored in the keystore under aliases. Each alias corresponds to a domain name, e.g. *webshare.yourserver.com*.

Certificates attempt to guarantee that a particular party is who they claim to be. Certificates are trusted based on who signed the certificate. If you only require light security, e.g. for internal use on trusted networks, etc. you can use “self-signed” certificates. Self-signed certificates encrypt the communication channel between client and server. However the client must verify the legitimacy of the self-signed certificate through some other channel as all current browsers reject self-signed certificates by default. Unfortunately, blindly accepting self-signed certificates opens up the system to “man-in-the-middle” attacks.

The advantage of self-signed certificates is that you can create them for free or for testing and evaluation. But as “LetsEncrypt” certificates are also free of charge, it is not worth using self-signed certificates¹. In addition, you can safely use a self-signed certificate if you can verify that the certificate you are using is legitimate. So if a system administrator creates a self-signed certificate, then

¹LetsEncrypt requires root access to the machine on which the WebShare Web Server is installed!

personally installs it on a client's truststore (so that the certificate is trusted) you can be assured that the SSL connection will only work between the client and the correct server.

For higher security deployments, you should get your certificate signed by a CA (*Certificate Authority*). Clients truststores will usually contain certificates of the major CAs and can verify that a CA has signed a certificate. This chain of trust allows clients to trust certificates from servers they have never interacted with before. Certificate signing is similar to a public notary (with equivalent amounts of verification of identity, record keeping, and costs).

7.4.3 Import an exiting certificate

The "wskeytool" utility (see 7.5 "wskeytool") allows importing certificates into the WebShare Web Server:

```
wskeytool -import -keyfile <private key> -file <public key> -trustcacerts
```

Example:

```
wskeytool -import -keyfile
           /etc/letsencrypt/live/example.com/privkey.pem
           -file /etc/letsencrypt/live/example.com/fullchain.pem
           -trustcacerts
```

If the private key file is encrypted, the `-keyfilepass` option must be specified. If private key and public key are stored in one file, the `-file` option must be omitted.

A documentation of all options is available using the following command:

```
wskeytool -import -h -v
```

Check the import:

```
wskeytool -list
```

The certificate should now be listed as "PrivateKeyEntry".

7.4.4 Request and import a new certificate from a CA

In order to configure SSL on your server you need to complete the following tasks:

1. Decide on your HELIOS WebShare Web Server domain
2. Create a key pair for your server domain certificate
3. Have a CA certify the SSL server certificate
 - a) Generate a CSR (*Certificate Signing Request*)
 - b) Submit your CSR to a CA for signing
4. Import the server certificate obtained from the CA into the keystore

Detailed instructions for each of the above steps:

1. Decide on your HELIOS WebShare Web Server domain

The WebShare Web Server domain should match the server hostname, e.g. “webshare.yourdomain.com”, the WebShare Web Server must be accessible under this domain name.

2. Create a key pair for your server domain certificate

In order to create a server certificate key pair, use the HELIOS “wskeytool” utility on the WebShare Web Server:

```
# cd /usr/local/helios/bin
```

Generate a key:

```
wskeytool -genkey -alias <WebShare Web Server domain>
```

Note: If you plan to change the CA for an existing certificate, just start with the following section. WebShare uses the existing certificate unless `-importcert` is called.

3. Have a CA certify the SSL server certificate

To get a CA signed certificate, you must first export the certificate to a file in the standard CSR format.

a) Generate a CSR:

```
wskeytool -certreq -file <CSR_filename>
```

b) Submit your CSR to a CA for signing.

4. Import the server certificate obtained from the CA into the keystore

If you had a CA sign your server certificate you must import it into your existing keystore:

```
wskeytool -importcert -file <signed_certificate_file> -trustcacerts
```

Important: The keystore must contain the complete certificate chain, from your domain certificate to the CA root certificate. Otherwise, the “websharewoa” service will not start up properly with HTTPS.

7.4.5 Create a certificate using an online CA (RFC 8555)

Prerequisite: port 80 needs to be accessible from the certification server (default: “https://acme-v02.api.letsencrypt.org”) under the WebShare Web Server domain and must not be used by another application.

```
wskeytool -acme -domain <WebShare Web Server domain> -contact <email>
```

7.4.6 Create a self-signed certificate

```
wskeytool -genkey -alias <WebShare Web Server domain>
```

Note: Will not be accepted by Internet browsers unless an an exception rule is defined.

7.5 wskeytool

“wskeytool” is a key and certificate management utility. Its purpose is to support the user in administration of the “HELIOS WebShare Web Server” keystore, required for HTTP/SSL support.

All command and option names are preceded by a minus sign (-). The options for each command can be provided in any order.

Commands:

-certreq

Generates a CSR using the PKCS#10 format. A CSR is intended to be sent to a CA. The CA authenticates the certificate requestor (usually off-line) and will return a certificate or certificate chain, used to replace the existing certificate chain (which initially consists of a self-signed certificate) in the keystore. The private key associated with `-alias` is used to create the PKCS#10 certificate request. If `-dname` is provided, then it is used as the subject in the CSR. Otherwise, the X.500 distinguished name associated with `-alias` is used. If `-ext` is provided, the extensions from the alias were replaced. The CSR is stored in the file “<file>”. If no file is specified, the CSR is output to “stdout”.

Note: Use the `-importcert` command to import the response from the CA.

Options:

- alias <alias>**
Alias name of the entry to process
- sigalg <alg>**
Signature algorithm name
- file <file>**
Output file name
- keypass <arg>**
Key password
- dname <name>**
Distinguished name
- ext <name:critical=value>**
X.509 extension
- keystore <keystore>**
Keystore name
- storepass <arg>**
Keystore password
- storetype <type>**
Keystore type
- v**
Verbose output
- q**
Suppress console output
- h**
Help output

-changealias

Move an existing keystore entry from the specified `-alias` to a new alias, `-destalias`. If no destination alias is provided, the command prompts for one. If no key password is provided, the `storepass` is attempted first. If this attempt fails, the user is prompted for a password.

Options:

-alias <alias>

Alias name of the entry to process

-destalias <alias>

Destination alias

-keypass <arg>

Key password

-cacerts

Access the CAcert keystore

-keystore <keystore>

Keystore name

-storepass <arg>

Keystore password

-storetype <type>

Keystore type

-v

Verbose output

-q

Suppress console output

-h

Help output

-delete

Deletes from the keystore the entry identified by `-alias`. The user is prompted for the alias, when no alias is provided at the command line.

Options:

-alias <alias>

Alias name of the entry to process

-cacerts

Access the CAcert keystore

-keystore <keystore>

Keystore name

-storepass <arg>

Keystore password

-storetype <type>

Keystore type

-v

Verbose output

-q

Suppress console output

-h

Help output

-exportcert

Reads from the keystore the certificate associated with `-alias` and stores it in the file "`<file>`". By default (if the `-rfc` option is not specified), the certificate is output in binary encoding. If `-alias` refers to a key entry with an associated certificate chain, the first certificate in the chain is returned. This certificate authenticates the public key of the entity addressed by `-alias`. If `-alias` refers to a trusted certificate, then that certificate is output.

Options:

- rfc**
Output in RFC style
- alias <alias>**
Alias name of the entry to process
- file <file>**
Output file name
- cacerts**
Access the CAcert keystore
- keystore <keystore>**
Keystore name
- storepass <arg>**
Keystore password
- storetype <type>**
Keystore type
- v**
Verbose output
- q**
Suppress console output
- h**
Help output

-genkeypair

Wraps the public key into an X.509 v3 self-signed certificate, which is stored as a single-element certificate chain. This certificate chain and the private key are stored in a new keystore entry identified by `-alias`.

The `-dname` value is used as the issuer and subject fields in the self-signed certificate.

Options:

- alias <alias>**
Alias name of the entry to process
- keyalg <alg>**
Key algorithm name
- keysize <size>**
Key bit size
- sigalg <alg>**
Signature algorithm name
- dname <name>**
Distinguished name
- ext <name:critical=value>**
X.509 extension
- startdate <date>**
Certificate validity start date/time
- validity <days>**
Validity number of days
- keypass <arg>**
Key password
- keystore <keystore>**
Keystore name
- storepass <arg>**
Keystore password
- storetype <type>**
Keystore type
- v**
Verbose output
- q**
Suppress console output

-h
Help output

-import

Reads the private key from a PKCS#1, PKCS#5, PKCS#8, or PKCS#12 formatted file and the certificate or certificate chain (where the latter is supplied in a PKCS#7 formatted reply or a sequence of X.509 certificates) from a second file, and stores it in the keystore entry identified by `-alias`. If neither `-keyfile` nor `-file` are specified, the certificate and private key are read from “stdin”. The data to be imported must be provided either in binary encoding format (DER) or in printable encoding format (PEM, also known as Base64 encoding) as defined by the Internet RFC#1421 standard.

The alias defaults to the first hostname found in the HELIOS preference **WOHost**. If this preference cannot be found, the default alias is built from the first “DNS” SubjectAlternativeName or from the X.500 distinguished name “CN” extracted from the certificate.

Options:

- noprompt**
Do not prompt
- trustcacerts**
Trust certificates from CAcert
- alias <alias>**
Alias name of the entry to process
- keyfile <file>**
Private key file name
- keyfilepass <arg>**
Source key password
- keyalg <alg>**
Key algorithm name

- file <file>**
Input file name
- keystore <keystore>**
Keystore name
- storepass <arg>**
Keystore password
- storetype <type>**
Keystore type
- v**
Verbose output
- q**
Suppress console output
- h**
Help output

-importcert

Reads the certificate or certificate chain (where the latter is supplied in a PKCS#7 formatted reply or a sequence of X.509 certificates) from `-file`, and stores it in the keystore entry identified by `-alias`. If no file is specified, the certificate or certificate chain is read from “stdin”.

“wskeytool” can import X.509 v1, v2, and v3 certificates, and PKCS#7 formatted certificate chains consisting of certificates of that type. The data to be imported must be provided either in binary encoding format or in printable encoding format (also known as Base64 encoding) as defined by the Internet RFC 1421 standard. In the latter case, the encoding must be bounded at the beginning by a string that starts with `---BEGIN`, and bounded at the end by a string that starts with `---END`.

You import a certificate for two reasons: To add it to the list of trusted certificates, or to import a certificate reply received from a

CA as the result of submitting a CSR to that CA (see the `-certreq` command). Which type of import is intended is indicated by the value of the `-alias` option.

If the alias does not point to a key entry, “wskeytool” assumes you are adding a trusted certificate entry. In this case, the alias should not already exist in the keystore. If the alias does already exist, “wskeytool” outputs an error because there is already a trusted certificate for that alias, and does not import the certificate.

If the alias points to a private key entry (or no alias is provided and there is exactly one private key entry in the keystore), “wskeytool” assumes you are importing a certificate reply. The public key from the certificate has to match that private key.

Options:

-noprompt

Do not prompt

-trustcacerts

Trust certificates from CAcert

-alias <alias>

Alias name of the entry to process

-file <file>

Input file name

-keypass <arg>

Key password

-cacerts

Access the CAcert keystore

-keystore <keystore>

Keystore name

-storepass <arg>

Keystore password

-storetype <type>

Keystore type

- v**
Verbose output
- q**
Suppress console output
- h**
Help output

-importkeystore

Imports one or all entries from another keystore (for import from PKCS#12, please note the differences to the `-import` command, which can also import an entry from PKCS#12, but the handling of the defaults is different).

If the `-srcalias` option is not provided, all entries in the source keystore are imported into the destination keystore. If a source keystore entry type is not supported in the destination keystore, or if an error occurs while storing an entry into the destination keystore, the user is prompted whether to skip the entry and continue or to quit.

If the destination alias already exists in the destination keystore, the user is prompted to either overwrite the entry or to create a new entry under a different alias name.

If the `-noprompt` option is provided, the user is not prompted for a new destination alias. Existing entries are overwritten with the destination alias name. Entries that cannot be imported are skipped and a warning is displayed.

The `-destalias` and `-srckeypass` options cannot be provided if the `-srcalias` option is not provided.

Options:

- srckeystore <keystore>**
Source keystore name
- destkeystore <keystore>**
Destination keystore name

- srcstoretype <type>**
Source keystore type
- deststoretype <type>**
Destination keystore type
- srcstorepass <arg>**
Source keystore password
- deststorepass <arg>**
Destination keystore password
- srcalias <alias>**
Source alias
- destalias <alias>**
Destination alias
- srckeypass <arg>**
Source key password
- destkeypass <arg>**
Destination key password
- noprompt**
Do not prompt
- v**
Verbose output
- q**
Suppress console output
- h**
Help output

-keyclone

Copy an existing keystore entry from the specified `-alias` to the new `-destalias`. If no destination alias is provided, the command prompts for one. If the original entry is protected with an entry

password, the password can be supplied with the `-keypass` option. If no key password is provided, `-storepass` is attempted first. If the attempt fails, the user is prompted for a password.

If the WebShare Web Server is connected via multiple hostnames, the command `-keyclone` can be used to copy an key entry into the alias for another hostname. The certificate must support this name (as wild card certificate or with an X.509 certificate extension “SubjectAlternativeName”).

Options:

- alias <alias>**
Alias name of the entry to process
- destalias <alias>**
Destination alias
- keypass <arg>**
Key password
- keystore <keystore>**
Keystore name
- storepass <arg>**
Keystore password
- storetype <type>**
Keystore type
- v**
Verbose output
- q**
Suppress console output
- h**
Help output

-list

Prints to “stdout” the contents of the keystore entry identified by `-alias`. If no alias is specified, the contents of the entire keystore

are printed.

By default, this command prints the common name (CN) and the SHA1 fingerprint of a certificate. If the `-v` option is specified, the certificate is printed in human-readable format, with additional information such as the owner, issuer, serial number, and any extensions. You cannot specify both `-v` and `-rfc`.

When retrieving information from the keystore, the password is optional. If no password is specified, the integrity of the retrieved information cannot be verified and a warning is displayed.

Options:

- rfc**
Output in RFC style
- alias <alias>**
Alias name of the entry to process
- cacerts**
Access the CACert keystore
- keystore <keystore>**
Keystore name
- storepass <arg>**
Keystore password
- storetype <type>**
Keystore type
- v**
Verbose output
- h**
Help output

-printcert

Reads the certificate from `-file`, the SSL server (`-sslserver`), or the signed JAR file (`-JAR_file`) and prints its contents in a human-readable format. Note that the `-jarfile`, `-sslserver`, and `-file` options cannot be provided at the same time. If neither option is specified, the certificate is read from “stdin”.

If the certificate is read from a file or “stdin”, it might be either binary encoded or in printable encoding format, as defined by the RFC 1421 Certificate Encoding standard.

Note: This command can be used independently of a keystore.

Options:

- rfc**
Output in RFC style
- file <file>**
Input file name
- sslserver <server[:port]>**
SSL server host and port
- jarfile <JAR_file>**
Signed JAR file
- help**
Help output

-printcertreq

Prints the content of a PKCS#10 format certificate request, which can be generated by the `-certreq` command. The command reads the request from `-file`. If there is no file, the request is read from “stdin”.

Note: This command can be used independently of a keystore.

Options:

-file <file>
Input file name

-v
Verbose output

-help
Help output

-printcrl

Reads the Certificate Revocation List (CRL) from `-file`. A CRL is a list of digital certificates that were revoked by the CA that issued them. The CA generates the file.

Options:

-file <file>
Input file name

-v
Verbose output

-help
Help output

-storepasswd

Changes the password used to protect the integrity of the keystore contents.

If a password file for the keystore exists, the user must have write access to it. The protection for key entries, protected with the keystore password (default, like WebShare Web Server certificates), changes to the new password.

Options:

-new <arg>
New password

-cacerts
Access the CAcert keystore

-keystore <keystore>
Keystore name

-storepass <arg>
Keystore password

-storetype <type>
Keystore type

-v
Verbose output

-h
Help output

When the `-v` option appears, it signifies verbose mode, which means that more information is provided in the output. This is also working in combination with the `-help` option.

7.5.1 Completion

➤ Restart the WebShare Web Server.

```
# srvutil stop websharewoa  
# srvutil start websharewoa
```

SSL setup is now complete and WebShare can be reached via both HTTP and HTTPS.

Note: To allow *only* HTTPS access and *not* HTTP, you must set the **WOPort** preference to 0 (see 7.6 “Preferences”).

7.5.2 Q & A

How will a “Certificate Request” look like?

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBxzCCATACAQAwgYYxCzAJBgNVBAYTAkRFMRAdgYDVQQIEwdHZXJt
YW55MRAdgYDVQQHEwdHYXJic2VuMR0wGwYDVQQKEXRIRUxJT1MgU29m
dHdhcmUgR21iSDEXMBUGA1UECXM0SEVMVSU9TIFN1...
-----END NEW CERTIFICATE REQUEST-----
```

Usually this needs to be submitted including the ---BEGIN. . . and ---END. . . lines into your CA (e.g. verisign.com)

Why is my browser telling me that the certificate does not match?

There can be several reasons for this:

- Your server domain name URL does not match the certificate
- Your certificate has not been signed by a CA
- Your certificate has expired
- Your browser does not know about your CA, e.g. VeriSign is installed in all major browsers

Our experience shows that Mozilla based browsers provide more detailed information on certificates than others. In a case of a problem these browsers can be used to show how the CA certificate response will look like.

7.5.3 Known issues

Problem:

If “websharewoa” issues an error message during startup:

```
websharewoa: [2009-11-28 15:54:30 MEST] <main> Unable to
establish an SSL connection to port 443 on this host
```

and then exits, make sure that the SSL port is not used by another application, e.g.:

```
# netstat -an | grep 443
```

should not list a line like below:

```
*.443 *.* 0 0 24576 0 LISTEN
```

Also check for the following message:

```
websharewoa: [2009-11-28 15:54:30 MEST] <main> com.webob-
jects.foundation.NSForwardException for com.webob-
jects.foundation.NSForwardException for
java.security.NoSuchAlgorithmException: Algorithm
SunX509 not available "Algorithm SunX509 not available"
```

indicates that the used JVM implementation does not offer SSL support. Check for an update to that JVM or install the Oracle JVM.

Problem:

The Microsoft Internet Explorer 6 cannot use a port other than 443 (default) for a “websharewoa” secure HTTPS connection.

7.6 Preferences

This section lists all the preference keys that are pertinent to the WebShare Web Server. Find a description of how to set, view, change or delete preferences, with the HELIOS “prefdump”, “prefvalue”, and “prefrestore” utility programs in “HELIOS utility programs” in the HELIOS Base manual.

Important: Make sure that preference keys *DO NOT* start or end with a slash (“/”) character, and note that they are case-sensitive! Also, if any preference key or preference value includes spaces, that key or value must be enclosed in quotes.

The following keys require a restart (see “*srvutil*” in the *HELIOS Base manual*) of the service to take effect:

Key: Programs/websharewoa/<preference>

WOPort int 2009

Specifies the WebShare Web Server port number for HTTP access. If set to “0” (without quotes) any HTTP connection to the WebShare Web Server is denied, only HTTPS/SSL connections are accepted. In that case, make sure the preference SSLPort is set, otherwise no connection to the WebShare Web Server can be established.

Note: If you wish to use HTTP port 80, and Apache or another web server is also running on the WebShare Web Server, see 10.1.11 “Switching WebShare to port 80 on the WebShare Web Server” for configuration details.

MDNSPort int 2006

Specifies the port number of the mDNS proxy server that is used for mDNS (“Bonjour”) branding registrations. If more than one WebShare Web Server is used, all used ports must have the same number.

Important: The value of this preference needs to be identical with the mDNS proxy server `TelnetPort` preference (see *HELIOS Base manual*). If there should be the need to change a value, then make sure that both preference keys are assigned the same value!

SSLPort int 443

Specifies the WebShare Web Server port number for HTTPS/SSL connections to the browser.

WOHost `str` (see description)

Specifies the hostname or IP address of the WebShare Web Server. This is useful on machines with multiple IP addresses/hostnames. If this preference is not set, the WebShare Web Server can be reached via any IP address/host name on the machine. The preference can also be set to a comma-separated list of IP addresses/hostnames. In addition, this preference allows specifying a port or SSL port, meaning that, if a port or SSL port is specified, the default settings (given by **WOPort** and **SSLPort**) are overridden.

Example 1:

```
(WOHost="myDomain:2035:2036"; WOPort="2009"; SSLPort="443");
```

For "myDomain", the default settings 2009 and 443 are overridden.

Access to the application:

```
http://myDomain:2035
```

and via SSL:

```
https://myDomain:2036
```

Example 2:

```
(WOHost="myDomain::2036"; WOPort="2009"; SSLPort="443");
```

For "myDomain", no individual port is specified so the standard settings apply.

Access to the application:

```
http://myDomain:2009
```

and via SSL:

```
https://myDomain:2036
```

Example 3:

```
(WOHost="myDomain:0:2036"; WOPort="2009"; SSLPort="443");
```

Specifying the port "0" for "myDomain" means that there are no standard (i.e. unencrypted and therefore insecure) connections available.

Access via SSL only:

```
https://myDomain:2036
```

WSRedirectToSSL `bool` `FALSE`

If set to `TRUE`, this preference induces the server to redirect the request to a secure Internet connection, for example:

`http://webshare.helios.de:2009 => https://webshare.helios.de:2012`

Note: It is required that an SSL port be specified via the **SSLPort** or **WOHost** preference.

WSDenyAccessForUA `strlist` `"+http"`

This preference contains a string list to specify user agents which should not be serviced. This is helpful to disable web crawlers that do not honor the “robots.txt”² file, e.g.:

```
prefvalue -k 'Programs/websharewoa/WSDenyAccessForUA' -t strlist
"+http://baidu.com,+http://webcrawlerXYZ.com"
```

Requests with a user agent string containing a string of this preference receive a status 404 (“not found”) response.

Important: A faulty entry, e.g. a string that is included in many user agents, can block access completely!

WSPublicHost `str` `""`

This preference determines which hostname is used by default when multiple network interfaces are active on the Webshare Web Server. Setting a public hostname may also become necessary if the internal WebShare Web Server hostname is different from that when used from external, e.g. via port mapping in a router/firewall, or via a proxy server. This setting is mainly used for Quickshare generated URLs. Two different settings are supported:

²“robots.txt” in the domain root allows defining the behavior of search robots on a website.

Qualified hostname: (e.g.: "webshare.yourdomain.com")

This specifies the hostname for public access when multiple network interfaces are valid. The port and SSL configuration will be used from the matching **WOHost** configuration with the `WSPublicHost` hostname specified.

URLs: (e.g.: "https://webshare.yourdomain.com:80")

Specifies the protocol, e.g. *http* or *https*, the hostname and, optionally, a port for generated public URLs. In this case, it must be ensured that public host connections are forwarded to the WebShare Web Server, e.g.:

<external hostname>:80 => <internal hostname>:2009.

WSDisabledSSLProtocols `strlist` "SSLv3, SSLv2Hello"

By default, this preference is not set which means that SSLv3 and SSLv2Hello are disabled. This configuration is advised by Oracle for all server applications supporting HTTPS.

The list of supported HTTPS protocols depends on the Java version.

Protocols supported by Java 7:

SSLv2Hello, *SSLv3*, *TLSv1*, *TLSv1.1*, *TLSv1.2*

If this preference is set, all protocols that should be disabled must be specified. Example configuration to allow TLSv1.2 and newer only:

```
prefvalue -k 'Programs/websharewoa/WSDisabledSSLProtocols' -t
           strlist "SSLv2Hello, SSLv3, TLSv1, TLSv1.1"
```

Note: Use this preference with care. Disabling additional protocols may cause incompatibilities with older web browsers using HTTPS.

WShostName `str` localhost, *

Specifies the WebShare File Server default hostname prompt for the login dialog. It corresponds to the `WebShare File Server` entry

in the WebShare login page. This preference can also be set to a comma-separated list of IP addresses or hostnames. In this case a pop-up menu to choose a WebShare File Server will be available at the login dialog.

Also aliases for IP addresses/hostnames can be defined:

```
prefvalue -k 'Programs/websharewoa/WSHostName' -t str
"localhost,Server 1=fileserver,Server 2=172.16.2.222"
```

In this case, a pop-up menu will be available to choose a WebShare File Server showing the strings “localhost”, “Server 1”, and “Server 2”.

It is also possible to specify a port number with the hostname, e.g.

```
prefvalue -k 'Programs/websharewoa/WSHostName' -t str
"localhost:2010,Server 1=fileserver,Server 2=172.16.2.222"
```

However, specifying a port number requires that this port has also been set, together with the hostname, in the `WSAllowedHostNames` preference, provided that `WSAllowedHostNames` was specified at all. If not, the connection is refused and an error message is issued.

If an “*” is found as a hostname in the `WSHostName` preference the user is allowed to enter a file server name manually, in addition to choosing a file server from the pop-up menu:

```
prefvalue -k Programs/websharewoa/WSHostName -t str
"localhost:2010,Server 1=fileserver,Server 2=172.16.2.222,*"
```

However, if more than one hostname or/and host alias are defined together with an “*”, JavaScript needs to be activated in the client application to get a pop-up menu displayed – otherwise a plain text field, showing the first defined hostname, is displayed.

If only one hostname or alias is defined, the user can neither choose nor enter a file server name.

The following examples give an overview of the possible cases:

Preference value: “*”

Display on login page: an empty text field.

Preference value: “localhost:2010”

Display on login page: the string “localhost:2010”.

Preference value: `"Server 1=localhost"`

Display on login page: the string "Server 1".

Preference value: `"localhost,*"` (default)

Display on login page: a text field with the value "localhost".

Preference value: `"Server 1=localhost,*"`

Display on login page: a text field with the value "Server 1".

Preference value: `"Server 1=localhost,otherhost"`

Display on login page: a pop-up menu with the values "Server 1" and "otherhost".

Preference value: `"Server 1=localhost,otherhost,*"`

Display on login page: a pop-up menu with the values "Server 1" and "otherhost", and in addition the ability to enter a file server name manually.

Note: If a list of file servers without an "*" is defined in the "WSHostName" preference, only file server names or file server aliases defined in this preference are accepted. However, if only one file server name or alias is defined – or an "*" is found as a host name – the file server name defined by the "wshost" parameter (see **wshost**) is used.

WSAllowedHostNames `str` (see description)

List of WebShare File Server hostnames or IP addresses which are allowed to be used on the WebShare Web Server. The string must be comma-separated if more than one "allowed" hostname or IP address is specified. If not set, all hostnames are allowed.

WSHostPort `int` 2010

Specifies the WebShare File Server port number. If more than one WebShare File Server is used, they all have to use the same port.

Note: The value of this preference needs to be identical with the WebShare File Server preference **TcpPort** (8.5 “Preferences”). If there should be the need to change a value, then make sure that both preference keys are assigned the same value!

WSUploadChunkSize `int64` 1024

This preference specifies the chunk size for drag & drop uploads in MB for uploads that exceed the 4 GB limit. Split uploads become necessary because of web browser and proxy server limits.

WSDisableHTML5Upload `bool` FALSE

If this preference is set to `TRUE`, the drag & drop upload functionality is switched off completely. Instead the standard upload form and window will be used.

WSEventDisplayPassword `str` ""

This preference allows specifying a password for a protected HTML page, which allows monitoring the WebShare Web Server and the events it is processing. By default, the page is unavailable until a password is set. For security reasons, this preference should not be used unless you are an WebObjects deployment specialist and you know how the WebShare Web Server and WebObjects work internally.

WSUpDownloadTimeOut `int` 86400

The default time-out value for uploads and downloads of the WebShare Web Server is 24 h (=86400 s). If more time is needed, e.g. due to a slow internet connection, this preference may be set to a higher value.

WOSessionTimeOut `int` 3600

Specifies that, after a user has been idle for a time, i.e. no web activity has occurred, the session will automatically be closed after one hour (=3600 s).

WSGZIPResponse `bool` `TRUE`

Modern browsers, e.g. Safari, Firefox, Internet Explorer support “gzip” compressed HTML pages. If supported by the browser, the WebShare Web Server generates “gzip” compressed HTML pages. For slow connections, e.g. via modem or ISDN lines this will increase the browsing performance by a factor of 2-5, depending on the content. In case of problems with compressed pages this feature can be turned off by setting this preference to `FALSE`.

WSPrintJavaExceptions `bool` `FALSE`

If this preference is set to `TRUE`, and an error occurs, a stack trace (debugging information) is printed on the error page.

JavaOptions `strlist` `""`

The values of this preference are passed through to the Java command when starting the “websharewoa” service. If specified, behavior, performance or debugging options can be set.

Note: Use this preference with caution! Providing invalid arguments will preclude “websharewoa” from starting! Providing wrong argument values can cause considerable performance issues.

7.6.1 WOStarter preference keys

WatchdogInterval `int` `600`

Specifies the interval in seconds in which the watchdog process checks the WebShare Web Server (“websharewoa”) for plausibility of its output to the web browser.

ResponsePositive `strlist` `""`

Specifies a list of strings that are mandatory in the WebShare Web Server response to the web browser if the behavior is normal. If

just one of these strings is missing, the “websharewoa” service is restarted. An example for a mandatory string is: “<!DOCTYPE html PUBLIC”.

ResponseNegative `strlist` ""

Specifies a list of strings that *must not* be contained in the WebShare Web Server response to the web browser. If just one of these strings is included, the “websharewoa” service is restarted.

8 WebShare File Server

“websharesrv” is the WebShare File Server, a native program running on the machine which can also host the HELIOS EtherShare/PCShare file servers, and is controlled by the HELIOS Service Controller (see HELIOS Base manual). It spawns a separate process for each user login.

The WebShare File Server offers various and versatile user and document management features, including e-mail notification on user login, additional customization in WebShare action scripts, etc.

8.1 User configuration file

“HELIOSDIR/var/conf/webshare.passwd” is the user configuration file of the WebShare File Server. Some specifications made on the “My User Preferences” administration page (see 6.7 “My User Preferences”) are stored in this file:

```
heliosuser:::zs=1,nocp=1,qs=1:::
martin:::zs=1,nocp=0,qs=0:::
ws1:md5_dd1c91f5d657b421c339592f:demo:::zs=1,nocp=1,qs=0:::
ws2:clr_clearpassword:demo:::zs=1,nocp=1,qs=1:::
```

Each line in “webshare.passwd” starts with the user name followed by several fields which are separated by colons. The first (user name) and third (user ID) field must be set, the other fields may remain blank.

User name

Virtual User or Host User

Password

(Password in clear text or MD5 hash code of UTF-8 clear text password)

A string starting with *md5_* is a crypted password for virtual users. A string starting with *clr_* is a hash value of the password for virtual users. For host users this field may be empty if there is no additional WebShare password set and the HELIOS host password is used. We recommend to set a different password, though.

Run as user

An empty field identifies a host user. For virtual users this field contains the name of the host user the virtual user is mapped to.

Expiry date

The 4th field contains the user expiry date/time in the format:

dd-*MMM*-yyyy-kk-mm

For example: **28-Feb-2004-14-21**

The Expiry date is entered in the `Expires` field on the "User Administration" page according to the syntax specified by the preference **DateFormat** (8.5 "Preferences").

Flags

(comma-separated)

"zs" (zipstream)

"nocp" (cannot change password)

"pt" (privileged transfer)

"br" (branding)=<branding name>

"po" (preview only for URL Share Access)

"qs" (Quickshare user)

Example:

If *zipstream* is enabled, this field shows "zs=1", otherwise "zs=0". If there is no entry, *zipstream* is enabled.

Client encoding

(for uploads/downloads)

Name of the client encoding for uploads/ downloads, e.g. “MacRoman”.

Empty when the “OS Default” has been specified.

E-mail address

This has to be a fully specified e-mail address, for example:

username@mycompany.com

Comment

Make sure that the comment does not contain special characters like a colon (“:”). These will be replaced with “_” in order to keep “webshare.passwd” compatible.

8.2 WebShare user settings file

User settings are stored in the “HELIOSDIR/var/run/WebShare_User_Settings/<user name>.settings” file (* = *PrintPreview* required):

```
* Application.session.annotationParameters
Default.preferredView
* Default.iccProfiles.printer
* Default.iccProfiles.monitor
* Default.iccProfiles.simulation
* Default.screen.width
* Default.screen.width.unit
* Default.screen.pixel
FileBrowser.session.showFileComments
FileBrowser.session.galleryIconSize
FileBrowser.session.searchResultView
FileBrowser.session.searchResultGalleryIconSize
FileBrowser.session.showGalleryDetails
* PrintPreview.zoom.originalSize
WSPrintDialog.settings.paperHeightSetting
WSPrintDialog.settings.marginWidthSetting
WSPrintDialog.settings.paperWidthSetting
WSPrintDialog.settings.resolutionValueString
WSPrintDialog.settings.bindingMargin
```

```
WSPrintDialog.settings.scaleImages
WSPrintDialog.settings.paperFormatString
WSPrintDialog.settings.unitName
* WSPrintDialog_ProofMode.settings.paperFormatString
* WSPrintDialog_ProofMode.settings.marginWidthSetting
* WSPrintDialog_ProofMode.settings.resolutionValueString
* WSPrintDialog_ProofMode.settings.controlGraphicPosition
* WSPrintDialog_ProofMode.settings.unitName
* WSPrintDialog_ProofMode.settings.bindingMargin
* WSPrintDialog_ProofMode.settings.paperHeightSetting
* WSPrintDialog_ProofMode.settings.scaleImages
* WSPrintDialog_ProofMode.settings.paperWidthSetting
* WSPrintDialog_ProofMode.settings.controlGraphicString
* WSPrintDialog_ProofMode.settings.printProofImageTitle
```

8.2.1 WSProperties

The “WSProperties” object allows getting and setting user settings (see 8.2 “WebShare user settings file”) or custom properties via JavaScript from the “additional.js” JavaScript file (see 4.7.9 “Customize brandings via JavaScript”). Custom properties will also be saved in the user settings file and provide a persistent way to save properties. If default user settings are saved (see **Save Default User Settings** in 6.7 “My User Preferences”) any custom properties will not be saved. “WSProperties” is implemented as a singleton and cannot be initiated. Note that the *getProperty* and *setProperty* methods may cause a read/write operation on the WebShare file server. If these methods should be executed asynchronously, set a callback function object with *setCallback*.

getProperty: function (<String> key)

Retrieve a property value for the given key. If the property is `null`, `false`, `true` or `undefined` it will be converted to a corresponding JavaScript object, otherwise a string is returned. If the property does not yet exist this method returns `null`.

key: The name of the property to retrieve.

setProperty: function (<String> key, <String> value)

Set a string property value for the given key. This method returns the new value of the property as it was retrieved via the *getProperty* method.

key: The name of the property to set.

value: The value the property specified with *key* should be set to.

setCallback: function (<Function> func)

Set a function object that will be called whenever the *readyState* attribute of the *XmlHttpRequest* object changes. If a callback function is set by this method the request will be performed asynchronously. The server response will be sent as an object notated in JavaScript Object Notation (JSON) format and contains the *propertyValue* object which will contain the value of the retrieved or set property. Use the JavaScript *eval* or *JSON.parse* function for parsing the JSON response inside the callback method.

func: A reference to a function object or an anonymous function which takes a *XmlHttpRequest* object as its argument.

8.3 WebShare utility programs

The “zipstream” and “unzipstream” programs are used for download and upload compression (and extraction). They are located in the “HELIOSDIR/bin” directory.

All other utilities described in this section are Perl scripts which are stored in “HELIOSDIR/etc/webshare”. For those scripts, the “dt” command will be used to ensure that all changes are applied to data and resource parts of files and folders. This ensures that HELIOS volume specific requirements are met.

Note: These Perl scripts can be customized. However, this should never be done in the original script file because it could be replaced during updates. Instead, copy the script from “HELIOSDIR/etc/webshare” into the “HELIOSDIR/var/webshare” directory. WebShare automatically looks first in “var/webshare” for all scripts and uses “etc/webshare” only as a fallback if the script is not available in “var/webshare”.

8.3.1 zipstream

This utility creates a Zip archive to which files and folders can be added in a compressed form. The advantages over the Zip program are that there are no temporary files created during compression, and file downloads can commence immediately without waiting for the archive to be created. Special file attributes like creation date, Mac type and creator and resource fork are encoded into MacBinary, which is preserved in the compressed Zip archive. UTF-8 is always the encoding used for file/folder name representation in the *file system*. The encoding used for file/folder name representation in the *Zip archive* can be specified to match the client computer system, e.g. MacRoman, PC850, ISO8859-1, UTF-8.

Due to the Zip64 support, files greater than 4 GB can be downloaded.

Usage:

```
zipstream [options] file
zipstream -h (for help info)
```

The following options are supported:

- f** Write the Zip archive to the file instead of writing to “stdout”.
- C** Input files are read from this directory.
- l** Zip compression level. Valid levels are from 1 (best speed) to 9 (best compression). The default level is 6.

- c** Encoding used for file names in Zip archive. The default encoding is UTF8. Use `unicconv -l` to list all available encodings (see HELIOS Base manual).
- “zipstream” is called with this option by the WebShare File Server when an encoding is selected via the `Download Encoding` pop-up menu on the “User Administration” or “My User Preferences” page.
-
- Note: The server volume encoding for “zipstream” is always assumed to be UTF-8. Non UTF-8 volumes are not supported.
-
- S** Print estimated Zip archive size to “stdout” (8 byte integer, network byte order).
- s** Print estimated Zip archive size to “stdout” (4 byte integer, network byte order).
- b** Write output in blocks of *n* kBytes. The default is 32 kB.
- n** No Zip streaming format.
- “zipstream” is called with this option by the WebShare File Server when the checkbox `Zip Streaming Format` is not checked.
- m** Encode the data and resource fork of a Mac file to MacBinary.
- p** Calculate precise Zip archive size (generates a temporary zip archive).
- t** Include file comments in MacBinary (works only together with the `-m` option).
- r** Preserve “.rsrc” directories. By default, “.rsrc” directories are skipped when creating the Zip archive. This option has no effect if `-m` is set.
- e** Add report file “DownloadLog.txt” to Zip archive containing file access errors and, if `-v` is also set, verbose information.

- v** Display verbose information on “stderr” or, if `-e` is also set, write verbose information to “DownloadLog.txt” in the Zip archive.
- z** Resolve symbolic links, add files into Zip archive.
- x** Generate OS X 10.3 (or newer) Finder compatible Zip archives, so that no additional archiving software is needed.
- i** Specify path to download accounting log file.
- o** Specify offset bytes to skip in data file. This option supports single file archives only for restarting downloads.
- N** Use the given file name for the Zip directory entry.
- d** Specifies the UTC (*Universal Time Coordinated*) time difference in seconds which is taken into account when generating dates within the Zip archive.
- u** Enforce Zip64 archive creation for entire Zip archive (otherwise it will automatically switch to Zip64 on archive sizes > 2 GB).
- w** Ignore `HideSpecialFiles` WebShare preference.

Example:

Create an Zip archive named “archive.zip” and add “file1”, “file2”, “dir1”, and “dir2” to the archive:

```
$ zipstream -f archive.zip file1 file2 dir1 dir2
```

8.3.2 unzipstream

The “unzipstream” utility expands Zip files and decodes MacBinary files.

By default, it reads a Zip or MacBinary file from “stdin”. The `-f` option can be used to specify a Zip or MacBinary input file. Output files are stored under

the names defined in the Zip or MacBinary file. If the input file is not a Zip or MacBinary file, it will be written to “stdout” or to the file specified by the `-o` option.

Usage:

```
unzipstream [options] file
unzipstream -h (for help info)
```

The following options are supported:

- f** Read the Zip archive instead of reading from “stdin”.
- o** Output file name. This is only used if the input file is not a Zip or MacBinary file.
- C** Output files are written to this directory.
- c** Encoding used for file names in Zip archive. The default encoding is UTF8.
Use `unicconv -l` to list all available encodings.

Note: The server volume encoding where Zip files are unpacked is always assumed to be UTF-8. Non UTF-8 volumes are not supported.

- r** Preserve “.rsrc” directories. By default, files in “.rsrc” directories are not extracted from the Zip archive.

Note: To prevent inconsistencies between information stored in the desktop database of a HELIOS volume and the files/folders on this volume, do not upload or extract a Zip archive with “.rsrc” directories directly into an active HELIOS volume. Make sure to use the HELIOS “dt” tools (see HELIOS Base manual).

-n <scriptname>

Name of a notification script that will be called after a file is extracted. The script is called with the following parameters:

- backupOriginal
- replaceOriginal
- directory
- temporary file name
- original file name
- file type (“Image” or “NoImage”)

-m Specify the MIME type of the input file. If **-m** is given, “unzipstream” does not check the header of the input file to determine the file type. Currently, two mime-types are supported: *application/x-macbinary* and *application/octet-stream*. If *application/octet-stream* is specified, “unzipstream” returns the input file unchanged.

-l List files instead of extracting them.

-u Unhide “dot files” by replacing the leading dot with an underscore.

Example:

.DS_Store is represented as *_DS_Store*.

-i Specify the path of the upload accounting log file.

-x <offset>

Specify *<offset>* bytes to skip in the target file before extracting. This option should only be used in combination with the **-t** option and single file archives to resume an interrupted upload.

-y <fileContentLength>

Specify the content length for uploads. The estimated upload length is verified to detect aborted uploads.

-t Specify the temporary upload file name. This is only used in combination with the **-x** option.

- b** If the file to extract already exists, backup the existing file. This option is only used with the “wsuploadmv” notification script. By default, “wsuploadmv” creates a different file (e.g. “file dup.txt”) if the file already exists.
- R** If the file to extract already exists, replace it. This option is only used with the “wsuploadmv” notification script. By default, “wsuploadmv” creates a different file (e.g. “file dup.txt”) if the file already exists.
- g <modtime>**
Specify a modification time for the extracted file. This option should be used with single file archives only.
- d** Specify the delta in seconds relative to UTC (*Coordinated Universal Time*).
- v** Display verbose information on “stderr”.
Please note that if a Zip file on its part contains Zip files in the archive, these will not be further expanded.

Examples:

List the Zip archive, assuming Windows (PC850) encoding:

```
$ unzipstream -l -c PC850 -f archive.zip
```

Extract the Zip archive which was created by DropZip, assuming Mac (MacRoman) encoding:

```
$ unzipstream -c MacRoman -f archive.zip
```

Extract all files in “abc.zip” to the directory “/data/zips”:

```
$ unzipstream -f abc.zip -C /data/zips
```

8.3.3 wscommon.pm

“HELIOSDIR/etc/webshare/wscommon.pm” is a Perl library module which is included by all WebShare Perl scripts. It contains, for example, information on other installed HELIOS products.

8.3.4 Action script environment variables

The following environment variables are available for WebShare action scripts or utility programs:

Environment variable	Description
<i>WSUserEncoding</i>	Download encoding; e.g. “OS Default”
<i>WSAccept-Language</i>	Currently used GUI language for WebShare; e.g. “en”
<i>WSWindowsEncoding</i>	Default Windows encoding; e.g. “PC850”
<i>WSStreamingZip</i>	Use Zip Streaming format; e.g. “Yes”
<i>WSMacintoshEncoding</i>	Default Mac OS encoding; e.g. “MacRoman”
<i>WSUserId</i>	Effective user ID of current session; e.g. “105”
<i>WSGroupId</i>	Effective group ID of current session; e.g. “30”
<i>WSUser</i>	Name of logged-in user
<i>WSUserEMail</i>	E-mail address of logged-in user
<i>WSSessionSeq</i>	websharesrv process ID (843) and number of logins (64); e.g. “843-64”
<i>WSClientAddress</i>	IP address of logged-in client
<i>WSPREVIEWDIR</i>	WebShare cache directory path
<i>WSUserAgent</i>	Browser information; e.g. “Mozilla/5.0 (Mac; U; PPC Mac OS X Mach-O; en-US; rv:1.6) Gecko/20040113”
<i>HELIOSDIR</i>	HELIOS directory path; e.g. “/usr/local/helios”

Note: The following environment variables are only available if the script is called from within a sharepoint via the `Actions >` menu:

Environment variable	Description
<code>WSSharepoint</code>	e.g. "Sample Images"
<code>WSSharepath</code>	e.g. "/template-images%0/"

8.3.5 wscopy.pl

Usage:

```
wscopy.pl destdir srcdir files...
```

This program is called by the WebShare File Server every time `Copy` or `Paste` function (in the `Edit >` toolbar menu) is selected. "destdir" specifies the destination directory, which the specified files and folders from the "srcdir" are copied to.

8.3.6 wsmove.pl

Usage:

```
wsmove.pl destdir srcdir files...
```

This program is called by the WebShare File Server every time the `Move` function (in the `Edit >` toolbar menu) is selected. "destdir" specifies the destination directory to which the specified files and folders from the "srcdir" are moved to.

8.3.7 wsdownload.pl

Usage:

```
wsdownload.pl zipstream-options offset srcdir files...
```

This program is called by the WebShare File Server every time the `Download` function is selected. “wsdownload.pl” uses the WebShare “zipstream” utility to stream an *on-the-fly* generated Zip archive without temporary files to “stdout”. With the “zipstream-options” argument additional options are passed on to a “zipstream” program call. The “offset” argument defines the number of bytes to be skipped for resuming single file archive downloads. The “srcdir” specifies the current directory of the user’s web session. The “files” argument consists of the files and folders that have been selected for download by the user. Settings like Zip format, file name encoding, MacBinary support, and client platform (Mac or Windows) are automatically determined by the “wsdownload.pl” script.

8.3.8 wsdup.pl

Usage:

```
wsdup.pl dir files...
```

This program is called by the WebShare File Server every time the `Duplicate` function (in the `File >` toolbar menu) is selected.

8.3.9 wsmkdir.pl

Usage:

```
wsmkdir.pl dir newdir
```

This program is called by the WebShare File Server every time the `Create Dir` function (in the `File >` toolbar menu) is selected.

8.3.10 wsmv.pl

Usage:

```
wsmv.pl dir source dest
```

This program is called by the WebShare File Server every time the `Rename` function (in the `File >` toolbar menu) is selected.

8.3.11 wspreview.pl

Usage:

```
wspreview.pl srcfile srcfiletype dstfiletype previewfile resOptions  
page antialiasPDF
```

This program is called by the WebShare File Server every time an image or document preview that is not yet available in the cache area, is requested from the client.

Parameters:**srcfile**

The complete path name to the image or document the user selected for preview.

srcfiletype

The file type of the document from which a preview is to be generated.

dstfiletype

The file type of the preview image; usually JPEG or PNG, see 6.4 "Generated previews" for details.

previewfile

The path name of the preview filename. The filename specifies the preview name to be saved in the preview cache area.

resOptions

This parameter specifies the preview options for the ImageServer “layout” command. Different parameters are split by a “|” character. For example,

```
-oxpix=256|-orotate=90|-oflipvertical
```

page

The page number starting with 1 used for multiple-page documents.

antialiasPDF

“True” or “False” to specify antialiasing for PDF input files.

8.3.12 wsforgotpw.pl

Note: This script does not require any user authentication.

Usage:

```
wsforgotpw.pl opts...
```

This program is called by the WebShare File Server every time the `Forgot Password?` link on the login page is clicked. The following table lists the Perl script field variables in the left column, and on the right the corresponding HTML field entries in the file “ForgotPassword.wod” (see 7.3.2 “Customizing “*.wod” files”). Please note that the Perl script variable names are given and cannot be renamed! If fields are not needed, leave them empty:

wsforgotpw.pl	ForgotPassword.wod
<code>\$username</code>	<code>editUser.username</code>
<code>\$email</code>	<code>editUser.email</code>
<code>\$organization</code>	<code>editUser.organization</code>
<code>\$comment</code>	<code>editUser.comment</code>
<code>\$field5 ... \$field10</code>	<code>editUser.field5 ... 10</code>

8.3.13 wsregnewuser.pl

Note: This script does not require any user authentication.

Usage:

```
wsregnewuser.pl opts...
```

This program is called by the WebShare File Server every time the `Register as a New User` link on the login page is clicked. The following table lists the Perl script field variables in the left column, and on the right the corresponding HTML field entries in the file “RegisterNewUser.wod” (see 7.3.2 “Customizing “*.wod” files”). Please note that the Perl script variable names are given and cannot be renamed! If fields are not needed, leave them empty:

wsregnewuser.pl	RegisterNewUser.wod
\$username	editUser.username
\$password	editUser.password
\$verifyPassword	editUser.verifyPassword
\$email	editUser.email
\$comment	editUser.comment
\$organization	editUser.organization
\$field7 ... \$field20	editUser.field7 ... 20

8.3.14 wsrn.pl

Usage:

```
wsrn.pl dir files...
```

This program is called by the WebShare File Server every time the `Delete` function (in the `File >` toolbar menu) is selected.

8.3.15 wsperm.pl

Usage:

```
wsperm.pl dir user group userMode groupMode otherMode recursive files
```

This program is called by the WebShare File Server every time the `Permissions` function (in the `File >` toolbar menu) is selected.

8.3.16 wsupload.pl

Usage:

```
wsupload.pl dstdir filesize backupOriginal replaceOriginal fileOffset  
tmpFilename filename mimetype
```

This program is called by the WebShare File Server every time the `Upload` function (in the `Transfer >` toolbar menu) is selected. “wsupload” receives the upload stream from “stdin” and unpacks the uploading stream in the directory specified by the “dstdir” parameter. The “unzipstream” utility is used as a back-end to unpack the data stream *on-the-fly*. As soon as a file within a Zip stream is detected, the file is saved with a temporary name with the process ID as suffix. For each file in the Zip stream the “wsuploadmv” script is called to rename the file with the process ID suffix to its final name. All this is done *on-the-fly* while “unzipstream” continues to receive data with additional files within the Zip stream. “wsupload” automatically detects if the upload is done from a Windows or Mac client, and will set up a proper character encoding according to the user and system settings.

8.3.17 wsuploadmv.pl

Usage:

```
wsuploadmv.pl backupOriginal replaceOriginal dir source dest  
backupOriginal and replaceOriginal can be set  
to '1' or '0'
```


This program renames uploaded files from their temporary name to their final name. “wsuploadmv” is a good place to add more processing tasks, e.g. a virus scanning software to verify uploaded files.

8.3.18 WebShare File Server service port

This service displays WebShare File Server user and status information.

- After calling `socket localhost` with the appropriate port on the command line, you may enter the additional commands `users`, `status` or `help` to display possible options:

```
$ socket localhost 2016
Welcome to the HELIOS WebShare File Server service port

help

help - print a list of available commands
quit - close connection
status - show status information
users - show user information
rmcache - remove all cache files

users

# PID      User UID Address      CRC      Login
1 inactive tom  101 192.168.1.2  24c9ce  Mon 10:38
1 active  joe  108 192.168.1.8  3bffc9d6 Thu 11:23
Summary: 1 active users (1 inactive users)

status

WebShare File Server, Version 4.0.0u1107
Up since: Wed Dec 3 10:25:30 2014
Max users: 0
Max users allowed: 65535
```

Note: For security reasons the WebShare File Server service port only accepts incoming connections from `localhost`. Remote access is not allowed.

8.4 WebShare scripts

8.4.1 Custom scripts

It is possible to include scripts in the WebShare workflow which automate tasks, etc. WebShare comes with some custom scripts (“wslogin.pl”, “wsaddshare.pl”, “wslogout.pl”, “wsemail.pl”, and “wspreviewaccess.pl”) that have to be customized by the user in order to take effect, and various sample action scripts (see 8.4.3 “Sample action scripts”). The custom scripts are stored in “HELIOSDIR/etc/webshare/samples”. In addition, the WebShare utility scripts in “HELIOSDIR/etc/webshare”, described in 8.3 “WebShare utility programs”, may also be customized.

Note: The standard output size of custom scripts is limited to 64 kB. However, the error output is limited to 2 kB.

Custom scripts become active after copied into the “var/webshare” directory.

wslogin.pl

This script is called after a successful WebShare login with the parameters:

- User name
- Apparent user IP address (If the user is e.g. “behind” a proxy server, the proxy IP address is presumed as user IP address)
- Complete browser identification string (*User Agent*)
- A string containing the user ID
- An options string containing the user type (*Virtual User* or *Host User*) as first entry; and separated by a comma the entry “IsAdmin”, if the user has Administrator rights

The script can be customized to perform any desired action upon a user login. A script return value of 0 would allow the user to log in to WebShare, whereas

a value different from 0 would deny the login, while issuing an error message via “stderr”.

Enhanced Document Hub security

This script can also be used for an enhanced Document Hub security by defining a list of mobile device IDs that are allowed to log on to the WebShare Web Server. A sample WebShare “wslogin.pl” script using Document Hub IDs can be downloaded from the HELIOS WebShare server:

```
Server:          webshare.helios.de
User name:      tools
Password:      tools
Sharepoint:    HELIOS Tools
Selection:     HELIOS WebShare > Sample wslogin.pl for DocumentHub IDs
```

wsaddshare.pl

Every time a WebShare Administrator adds or modifies a sharepoint, the “wsaddshare.pl” script is called. Its parameters are:

- Sharepoint name
- Sharepoint path
- Sharepoint e-mail address
- An options string with the boolean preferences of the sharepoint (**Publish**, **AllowDownload**, etc.) containing the sharepoint preference keys in a comma-separated list
- A list of all users who are allowed to see the sharepoint
- A list of all groups whose user members are allowed to see the sharepoint

By customizing this script, a System Administrator can prevent WebShare Administrators from creating a sharepoint whose path points beyond the administrative (allowed) area. A return value of 0 would allow creating a sharepoint or applying changes in a sharepoint, whereas a value different from 0 would deny these actions, while issuing a message to the System Administrator via “stderr”.

wslogout.pl

As soon as the user has logged out, this script is called with the following parameters:

- User name
- HTTP client TCP/IP address
- Complete browser identification string (*User Agent*)

This script may be customized, e.g. to clean up directories or to accomplish similar tasks. In contrast to **wslogin.pl** and **wsaddshare.pl**, the return value of this script is not interpreted.

wsemail.pl

This action script is called every time a user sends an e-mail via WebShare. The script is called with the parameters:

- User name
- Recipient (field `To:`)
- Carbon copy recipient (field `CC:`)
- Blind carbon copy recipient (field `BCC:`)
- Subject
- Mail text

The Script must exit with status 0 to allow the user sending e-mail or status 1 to deny sending an email.

wspreviewaccess.pl

If a script named “wspreviewaccess.pl” is copied to “HELIOSDIR/var/webshare” it is called every time an image preview is requested.

The script has two arguments:

1. `<Pathname>` to the image
2. `<Pathname>` to the cache preview file

This allows precise auditing for third-party scripts which may use this information to get informed about the preview activities.

8.4.2 Debugging WebShare scripts

All WebShare scripts are developed in Perl including the sample scripts. They can be developed in any language, e.g.: shell, PHP, Perl, Java, C/C++. HELIOS prefers Perl because it is very powerful and compatible across different server platforms. This chapter provides guidelines on how to debug Perl scripts to be used as utility and action scripts within WebShare. Make sure to implement and debug your script so that it works in general before you begin debugging it in the WebShare environment.

Environment requirements:

All scripts are called with the current working directory HELIOSDIR, which is “/usr/local/helios” by default. To be compatible on all platforms without depending on the Perl installation path all WebShare Perl scripts include a `#!/var/run/runperl` in the first line. “runperl” is a symbolic link to the local Perl interpreter. The “runperl” link is automatically created during the WebShare installation. All WebShare default scripts are included in “etc/webshare”. Customized scripts should be stored in “var/webshare” to avoid overwriting your scripts during a new installation. Another benefit is that the entire “var” folder contains all customization and settings, which allows easy migration to a different server platform without applying all changes again.

Printing debugging information:

As many scripts produce their output to “stdout” or “stderr”, printing script variables will produce mixed output which leads to malfunctions. All HELIOS scripts support debug output into a file by specifying the “DEBUGTTY” environment variable.

A simple debugging session:

```
# cd /usr/local/helios
# export DEBUGTTY=/dev/tty
# var/webshare/actions/<yourscriptname>
```

The above commands allow to test drive the script and to check the results.

A debugging session within a running WebShare File Server:

```
# cd /usr/local/helios
# bin/srvutil stop websharesrv # to stop the webshare file server
# export DEBUGTTY=/dev/tty
# sbin/websharesrv
```

The manual start of the WebShare File Server as shown above prints all output into the current terminal.

8.4.3 Sample action scripts

As mentioned in 8.4.1 “Custom scripts”, WebShare comes with various sample action scripts:

- wsannotations.pl (*List annotations*)
- wscmdargs.pl (*Cmd ARGS*)
- wsdialog.pl (*Dialog sample*)
- wsdu.pl (*Disk usage*)
- wsimageinfo.pl (*Image info*)
- wslinks.pl (*WebShare link example*)
- wsl.pl (*ls -l*)
- wspdfinfo.pl (*PDF info*)
- wssendmsg.pl (*Send message*)
- wsspotlightmeta.pl (*Spotlight metadata*)
- wsxpvcollect.pl (*Collect files from XPV*)
- wsxpvinfos.pl (*XPV info*)

The string entered in the script header, in the line `#Title=`, is used as the script title in the menu.

Located in “`var/settings/WebShare/Actions/Samples`”, the scripts must be copied to “`var/settings/WebShare/Actions`” in order to become available in the `Actions >` pop-up menu in the toolbar of the sharepoint window (see section **Actions >** in 6.3 “Work in a sharepoint”). In addition, the file access permissions of each action script determines if it is even visible to individual users. See 10.1.7 “Action scripts”.

wsannotations.pl

This action script returns a table of all annotations for the current sharepoint, and offers a search functionality for annotations.

wscmdargs.pl

This action script prints out the script arguments and the environment variables.

wsdialog.pl

This two-step action script first generates a form with customized HTML fields (text fields, buttons, etc.), which are then processed.

wsdu.pl

Action script to show disk usage of files by use of the `du` command.

wsimageinfo.pl

(*ImageServer required*) Action script to extract information about an image.

wslinks.pl

This action script allows opening the WebShare components *file browser*, *preview*, *proof*, *download*, *Spotlight search*, *upload* to dynamically create HTML hyperlinks, to enable the user to navigate to different WebShare components. For example, navigate into a proof window which displays page 12 of a specified file, with a zoom of 100%.

wsl.pl

This action script lists, by use of the `ls -l` command (on Windows `dir`), the content of the current directory.

wspdfinfo.pl

(*PDF HandShake required*) Action script to extract information about a PDF document.

wssendmsg.pl

Action script to send messages from WebShare to all users that are connected via “afpsrv”, “pcshare” or “heladmsrv”.

wsspotlightmeta.pl

Action script which returns a table of Spotlight metadata for all selected files.

wsxpvcollect.pl

(*ImageServer required*) Action script to collect the referred data (QuarkXPress or InDesign document and images) from the XPV document. It creates also a report about the used fonts.

wsxpvinfo.pl

(*ImageServer required*) Action script to extract information about an XPV document.

Note: If the name of the script file starts with “hide-” (e.g. “hide-scriptname.pl”) the script will not be listed in the `Action >` menu of the toolbar. This is useful for actions that will be called by JavaScript (see 8.4.4 “Calling action scripts via JavaScript”) but should not be visible for the user.

8.4.4 Calling action scripts via JavaScript

It is possible to call any custom action script via JavaScript from the “additional.js” JavaScript file (see 4.7.9 “Customize brandings via JavaScript”). This allows customization of workflows or adding new features and options. To call a custom action script via JavaScript make use of the *WSJavaScriptCommand* object. Custom actions can be called from the WebShare “Home” page, the file browser page, the preview page, the proof window, the “Administration” page, and the “My User Preferences” component.

To call custom action scripts from JavaScript use the *WSJavaScriptCommand* object. It contains the following public methods:

addFiles: function (<Array> or <Object> files)

Add files to the action script as if they were selected in the file browser.

files: An array of HTML element objects or a single HTML element object like *HTMLTableRowElement*, a *HTMLTableCellElement*, or similar.

addParameters: function (<Object> parameters)

The key/value pairs of the given object will be passed to the action script as “POST” variables. If any name field content has been set via the *setNamefieldContent* method this method will throw a *WSJavaScriptCommandException*.

parameters: An object holding key/value pairs.

send: function ()

Sends the request. If no command name has been set via the *setCommand* method this method will throw a *WSJavaScriptCommandException*.

Returns: `true` if the request has been sent, `false` if no request can be sent from the current component.

setCallback: function (<Function> func)

The function object `func` will be called whenever the *readyState* attribute of the *XmlHttpRequest* object changes. The *XmlHttpRequest* object will be passed as a parameter to the function.

`func`: A reference to a function object or an anonymous function which takes a *XmlHttpRequest* object as its argument.

setCommand: function (<String> name)

Set the name of the script to invoke.

`name`: The name of the action script to invoke, e.g. “wsannotations.pl”.

setNamefieldContent: function (<String> content)

Set the content of the name field of an action. If any “POST” parameters have been set via the *addParameters* method this method will throw a *WSJavaScriptCommandException*.

`content`: The content of the name field of an action script.

setSharepoint: function (<String> name)

Sets the name of the current WebShare sharepoint. In the “File-Browser”, “Preview”, and “Proof” components, the sharepoint name cannot be overridden and this method will throw a *WSJavaScriptCommandException* if invoked. It should be used to set a sharepoint in components that do not have a sharepoint context like the “Administration” component. You may want to call this method within a try/catch block.

`name`: The name of a WebShare sharepoint.

8.5 Preferences

This section lists all the preference keys that are pertinent to the WebShare File Server. Find a description of how to set, view, change or delete preferences, with the HELIOS “prefdump”, “prefvalue”, and “prefstore” utility programs in “HELIOS utility programs” in the HELIOS Base manual.

Important: Make sure that preference keys *DO NOT* start or end with a slash (“/”) character, and note that they are case-sensitive! Also, if any preference key or preference value includes spaces, that key or value must be enclosed in quotes.

Key: Programs/websharesrv/<preference>

8.5.1 WebShare File Server preference keys

WrongAuthDelay int 2

Specifies the time delay in seconds between failed login requests. This helps increase the security against unauthorized logins, e.g. by password robots, which try to match the password by issuing a large number of passwords per second.

AllowForgotPassword bool FALSE

Determines whether the `Forgot Password?` link becomes visible in the login window. The setting of this preference reflects the state of the `Enable Forgot Password Option` checkbox on the “Server Preferences” page (Fig. 4.3).

AllowRegisterUser bool FALSE

Determines whether the `Register as a New User` link becomes visible in the login window. The setting of this preference reflects the state of the `Enable Register User Option` checkbox on the “Server Preferences” page (Fig. 4.3).

AllowEmailMessages bool TRUE

Determines whether the `Mail` function (in the `Edit >` toolbar menu) is available. The settings of this preference reflects the setting of the `Enable E-Mail message for Users` checkbox on the “Server Preferences” page (Fig. 4.3).

EnforceCryptedLogin bool FALSE

With this preference set to `TRUE`, only encrypted user logins are permitted (JavaScript must be active in the web browser). The setting of this preference reflects the state of the `Enforce RSA Crypted Passwords` checkbox in the “Server Preferences” page (Fig. 4.3).

AllowLinkShares bool FALSE

With this preference set to `TRUE`, WebShare allows direct URL access from remote clients.

AllowQuickshares bool FALSE

Set this preference to `TRUE` to allow Quickshares. The setting reflects that of the `Allow Quickshares` checkbox in the “Server Preferences” page (Fig. 4.3).

GlobalQuickshareUsers bool FALSE

With this preference set to `TRUE`, *all* Quickshare users are available in the `Quickshare User` pop-up menu. The setting reflects that of the `Quickshare Users Are Global` checkbox in the “Server Preferences” page (Fig. 4.3).

QuickshareEmptyPassword bool FALSE

With this preference set to `TRUE`, a remote user is allowed to open Quickshare links by just clicking on them, without the need to previously log in on the WebShare server (requires an empty password). The setting of this preference reflects the state of the `Skip Login With Empty Quickshare Passwords` checkbox in the “Server Preferences” page (Fig. 4.3).

The following keys require a new login to take effect:

AnnotationPrefix `str` `""`

If an annotation is added to a file in the preview or proof window, it is named “<file name>.annotation” and saved adjacent to the original file. This preference allows specifying prefixes for the annotation file, e.g. a dot (“.”), which would hide the file in the WebShare file browser. Also directories can be specified; if “anno/” is specified, the annotation file is saved to the directory “anno” which is created adjacent to the original file.

DisableUTCDelta `bool` `FALSE`

Allows deactivating the time adjustments. The default is `FALSE` which means time zones are automatically adjusted.

MaxWoaBlockSize `int` `128`

This value is specified in kilobytes. The WebShare protocol block size between the WebShare Web Server and the WebShare File Server specifies the maximum size of a command (except for downloads, uploads, and previews, which are streamed). For example, if annotations become larger than 128 kB, this parameter allows increasing the maximum block size to a higher value.

URLSuffixSize `int` `8`

For QuickShare tiny URLs this parameter describes how many random bytes are used in the URL to avoid that anonymous users can try out QuickShare URLs by entering all combinations. The default is 8, with a minimum of 2 and a maximum of 254.

logdenied `bool` `FALSE`

If set to `TRUE`, this parameter lets “websharesrv” append a record to the system messages if, due to the IP access list, access to one or more users has been denied.

MaxGalleryRes `int` 384

This preference specifies the maximum resolution for image previews in the gallery view. If the value of the preference is set to 0, the gallery view mode is not available (the corresponding button in the `File > Set View > Gallery` menu is grayed out or hidden, depending on the `Show Disabled Buttons` setting of the used branding, see **Toolbar** in 4.7.1 “Create and configure brandings”).

If the specified value is less than 32 the WebShare Web Server assumes 32 as the maximum size.

TcpRecvSize `int` 65536 (64 x 1024)

Specifies the maximum number of TCP data bytes that are passed from the clients to “websharesrv” over the network during a transaction. The number of bytes may need to be limited if the buffer size in the UNIX server is too small. `TcpRecvSize` can be varied to optimize the data transfer rate.

TcpSendSize `int` 65536 (64 x 1024)

Specifies the maximum number of TCP data bytes that are passed from “websharesrv” to the clients over the network during a transaction. The number of bytes may need to be limited if the buffer size in the UNIX server is too small. `TcpSendSize` can be varied to optimize the data transfer rate.

Note: Changed values in `TcpRecvSize` and `TcpSendSize` will automatically be assigned to the WebShare Web Server as well, for the next login.

CacheSize `int` 30 (in MB)

Specifies the cache size value of the WebShare File Server for preview files. It corresponds to the Cache Size in MB value in the WebShare “Server Preferences” menu.

Note: The default value for `CacheSize` is 30 (MB), due to the usually limited disk space in “HELIOSDIR/var”. If you change the `CacheDir` preference to another path, it is recommended to set `CacheSize` to a value of at least 300 (MB).

AllowHostUsers `bool` `TRUE`

Specifies whether users are allowed to log on to the WebShare File Server with their host login name. The setting reflects that of the `Enable WebShare for Host Users` checkbox in the Webshare “Server Preferences” menu.

AllowVirtualUsers `bool` `TRUE`

Specifies whether users are allowed to log on to the WebShare File Server with their (virtual) WebShare login name. The setting reflects that of the `Enable WebShare for Virtual Users` checkbox in the Webshare “Server Preferences” menu.

AdminNotify `str` `""`

Specifies an e-mail address to which a notification is sent as soon as a client with Admin rights logs on to the WebShare File Server. It corresponds to the `E-Mail Notification on Admin Login` entry in the Webshare “Server Preferences” menu.

Note: Make sure that the complete receiver account is specified, e.g. **webshare@mycompany.com**

UserNotify `str` `""`

Specifies an e-mail address to which a notification is sent as soon as a user logs on to the WebShare File Server. It corresponds to the `E-Mail Notification on User Login` entry in the Webshare “Server Preferences” menu.

Note: Make sure that the complete receiver account is specified, e.g. **webshare@mycompany.com**

AllowAllReadWrite `bool` `FALSE`

If set to `TRUE`, this preference enables the sharepoint preferences **AllRead** and **AllReadWrite**. In that case, the additional options `Always Allow Reading` and `Always Allow Read/Write` (see 8.5.2 “Sharepoint preference keys”) will be shown in the “Sharepoint Administration” page.

Important: It may considerably reduce host security to set the `AllowAll-ReadWrite` flag to `TRUE` because if required, host access rights are bypassed, with all user processes changing to “root” processes!

DateFormat `str` `"dd MMM yyyy kk:mm"`

Specifies the format with which the date is displayed in the file browser of the “Sharepoint” menu. It corresponds to the `Directory Listing Date Format` entry in the Webshare “Server Preferences” menu. Also, this preference specifies the required syntax for the `Expires` field in the “User Administration” page. See **Date format** in 4.1 “Server Preferences”.

ProofProfiles `str` `"CromalinEuro 1.0 UCR370,..."`

Specifies those profiles from the “ICC-Profiles” volume that should be available in the `ICC Proof Simulation` pop-up menu in the WebShare proof window.

AllowUserICCProfiles `bool` `FALSE`

If this preference is set to `TRUE`, WebShare users are allowed to upload and administer their own monitor and printer ICC profiles

on the “My User Preferences” administration page. It corresponds to the `Allow ICC Profiles per User` entry in the WebShare “Server Preferences” menu.

mail `bool` `TRUE`

Specifies whether e-mail notification is used at all.

SendMailOnActionScript `bool` `FALSE`

If set to `TRUE`, this preference sends an e-mail, as soon as a WebShare action script is executed, to the address that is specified in the `Email on Access` field on the “Sharepoint Administration” page. See **EmailAccess**.

DefaultWindowsEncoding `str` `"PC850"`

Specifies the default encoding method when downloading files on Windows clients. The setting reflects that of the `Default Windows Encoding` pop-up menu on the “WebShare Server Preferences” menu.

DefaultMacintoshEncoding `str` `"MacRoman"`

Specifies the default encoding method when downloading files on Mac clients. The setting reflects that of the `Default Mac OS Encoding` pop-up menu in the WebShare “Server Preferences” menu.

ShowHiddenFiles `bool` `FALSE`

If set to `TRUE`, hidden files (“dot files” and files which have been marked as *hidden* in an EtherShare volume) are displayed in a sharepoint file browser.

HideSpecialFiles `strlist` `""`

Specifies file names which should always be hidden in a directory listing.

PreviewResolutions `str` (see description)

Specifies the (comma-separated) pixel/resolution values which are available in the “Sharepoint” preview pop-up menu. The “zoom

icon” resolution values are defined in the “Branding Editor > *Branding* > Preview Resolutions 1-4” preference, and are not affected by this preference.

By default, the following resolutions are available:

36 dpi,72 dpi,96 dpi,144 dpi,128 pixel,256 pixel,512 pixel,
768 pixel,1024 pixel

CustomPreviewTypes `str` `""`

Allows specifying suffixes for custom file types that are to be previewed in WebShare and which must be processed first (according to the rules given in the “wspreview.pl” script). For example, `doc, xls, ppt` (no blanks!) can be specified for Microsoft Office documents which, if required, are processed by Tool Server with the “OfficeReader” script.

URLWebOnlyUsers `strlist` `""`

If this preference is set, the specified users have only URL based WebShare web access. See also the **AllowLinkShares** preference.

URLImageOnlyUsers `strlist` `""`

If this preference is set, the specified users have only URL based WebShare image fetching access. This allows setting up a special user (real or virtual) for remote URL image-only access. If somebody tries to steal the URL specified user name and password for a manual WebShare login, this will be denied. See also the **AllowLinkShares** preference.

Important: Specifying the same user name(s) with both preferences **URLWebOnlyUsers** and **URLImageOnlyUsers** will cause that the access for the specified user(s) is denied at all – be it via URL Share Access or manual login. So make sure to use different user names with both preferences!

*The following keys require a restart (see “`srvutil`” in the *HELIOS Base manual*) of the service to take effect:*

MaxUsersLimit `int` `see description`

Allows limiting the WebShare user count. The “Universal File Server” license allows access from EtherShare, PCShare, and WebShare. Each service counts against the “Universal User” count. So it is possible that many WebShare users use up all available user licenses, so that no EtherShare or PCShare login is possible anymore.

Note: Starting with 60 “Universal Users”, WebShare can be used with unlimited users. In this case, WebShare users do not affect EtherShare or PCShare logins, so it makes no sense to set this preference.

TcpPort `int` `2010`

Specifies the WebShare File Server port number. Additional TCP ports (up to a total of five) will automatically be allocated as needed by the WebShare File Server.

Important: The value of the `TcpPort` preference needs to be identical with the WebShare Web Server preference **WSHostPort** (7.6 “Preferences”). If there should be the need to change a value, then make sure that both preference keys are assigned the same value!

TelnetPort `int` `2016`

Specifies the “telnet” service port number of the WebShare File Server.

sessions `int` `(see description)`

Specifies the maximum number of workstations (clients) that are permitted to work on the WebShare File Server simultaneously.

This value should normally be the same as the total number of workstations that are connected to the WebShare File Server, and should be less than or equal to the number of `sessions` allowed by your software license. The default value for `sessions` is the number of sessions allowed by your software license.

minuid `int` (see description)

Specifies the lowest number allowed for user IDs. All host users which have a lower user ID than that specified by `minuid`, and all virtual users running as a host user with a user ID lower than that specified by `minuid`, are not permitted to log in. The default behavior is that all IDs are allowed.

maxuid `int` (see description)

Specifies the highest number allowed for user IDs. All host users which have a higher user ID than that specified by `maxuid`, and all virtual users running as a host user with a user ID higher than that specified by `maxuid`, are not permitted to log in. The default behavior is that all IDs are allowed.

ipaccess `str` "ipaccess"

Specifies the file containing the access list with the IP addresses which are permitted to log on to "websharesrv". See HELIOS Base manual.

CacheDir `str` "var/tmp/wscache"

Specifies the directory which contains the preview files on the WebShare File Server. It corresponds to the `Cache Directory` entry in the "WebShare Server Preferences" menu.

Note: This directory must already exist and have `rwX` (read-write-execute) permissions for all.

AliasPDF bool TRUE

If set to `FALSE`, antialiasing for PDF previews is deactivated.

8.5.2 Sharepoint preference keys

The following keys take effect immediately:

Key: `Programs/websharesrv/Shares/<sharename>/<preference>`

Path str ""

Specifies the sharepoint path. It corresponds to the `Sharepoint Path` entry in “Sharepoint Administration”.

Publish bool TRUE

Specifies whether a sharepoint is published in the “Home” menu. The setting reflects that of the `Publish` checkbox in the “Sharepoint Administration” page.

EmailAccess str ""

Specifies an e-mail address for notification mails on user access and action to the selected sharepoint. It corresponds to the `Email on Access` entry on the “Sharepoint Administration” page. Make sure that the complete receiver account is specified, e.g. `webshare@mycompany.com`.

CollectMails bool TRUE

Specifies whether user action notification mails, as stated in the `EmailAccess` preference, are issued after the user has logged out, which is the default behavior, or – if set to `FALSE` – immediately after each file download, upload or deletion done by a user.

Note: If set to `FALSE`, no notifications for *previews* are issued at all because this would result in a flood of notification mails.

AllowCopy bool FALSE

Specifies whether copying files to the sharepoint and creating directories is allowed. The setting reflects that of the `Allow Copy` checkbox on the “Sharepoint Administration” page.

AllowDelete bool FALSE

Specifies whether deleting files in the sharepoint is allowed. The setting reflects that of the `Allow Delete` checkbox on the “Sharepoint Administration” page.

AllRead bool FALSE

Specifies whether file read access in the sharepoint is enabled for all users, irrespective of the server file access settings. Read access includes file download and preview. The setting reflects that of the `Always Allow Reading` checkbox on the “Sharepoint Administration” page. This preference must first be enabled by the WebShare administration preference key **AllowAllReadWrite**.

AllReadWrite bool FALSE

Specifies whether file read/write access in the sharepoint is enabled for all users, irrespective of the server file access settings. Read/write access includes file download, upload and preview. The setting reflects that of the `Always Allow Read/Write` checkbox in the “Sharepoint Administration” page. This preference must first be enabled by the WebShare administration preference key **AllowAllReadWrite**.

OnlyLayouts bool FALSE

If set to `TRUE`, only layouts of the images in the sharepoint can be downloaded. The setting reflects that of the `Download Layouts only` checkbox in the “Sharepoint Administration” page. For this preference to be enabled, the WebShare File Server preference **AllowDownload** must be set to `TRUE`.

Users `strlist` `" "`

Specifies one or more user names for which the sharepoint is available. If no names are specified, the sharepoint is available for all users. It corresponds to entries in `Allowed Users` on the “Sharepoint Administration” page.

Groups `strlist` `" "`

Specifies one or more group names for whose members the sharepoint is available. If no names are specified, the sharepoint is available for all groups. It corresponds to entries in `Allowed Groups` on the “Sharepoint Administration” page.

For WebShare, the sharepoint (volume) key is the name of the sharepoint, for example “WebShare Public”, whereas for EtherShare and PCShare the volume key is the directory path, for example “/demovol”.

To set up a sharepoint “Mycompany Public”, similar to the “WebShare Public” by using “prefvalue”, the following prefvalue sequences must be called:

```
# prefvalue -k "Programs/websharesrv/Shares/Mycompany Public/
Path" -t str "/mycompany/public/WebShare"

# prefvalue -k "Programs/websharesrv/Shares/Mycompany Public/
AllowDownload" -t bool TRUE

# prefvalue -k "Programs/websharesrv/Shares/Mycompany Public/
AllowPreview" -t bool TRUE
```

By default, the **Publish** flag is set, therefore it need not be specified.

8.5.3 Quickshare preference keys

The following keys require a new login to take effect:

```
Key: Programs/websharesrv/Quickshares/<QS #>/<preference>
```

- | | | |
|-------------------|--|-------|
| Active | bool | FALSE |
| | Specifies if a Quickshare is active. Setting a Quickshare status to FALSE, does not mean that the Quickshare is deleted but it is not available for remote users. The setting reflects that of the <code>Active</code> checkbox on the “Quickshare Administration” page. | |
| Username | str | " |
| | Specifies the name of the WebShare user to whom the Quickshare was assigned. The setting reflects the first part of the content of the <code>Quickshare User</code> pop-up menu on the “Quickshare Administration” page. | |
| Sharepoint | str | " |
| | This preference states the WebShare sharepoint that a Quickshare points to. The setting reflects the content of the <code>Sharepoint</code> text field on the “Quickshare Administration” page. | |
| Path | str | " |
| | This preference states the path that a Quickshare points to. The setting reflects the content of the <code>Path</code> text field in the “Quickshare Administration” page. | |
| Expires | uint32 | 0 |
| | This preference allows you to enter an expiry date after which the Quickshare becomes void. The setting reflects the content of the <code>Expires</code> text field on the “Quickshare Administration” page. | |

- Comment** `str` `""`
- This preference allows you to enter a comment for the remote Quickshare user. The setting reflects the content of the `Comment` text field on the “Quickshare Administration” page.
- Creator** `str` `""`
- This preference states the creator of a Quickshare. The setting reflects the content of the `Creator` text field on the “Quickshare Administration” page.
- CreatorEMail** `str` `""`
- Specifies the e-mail address of the logged-in user who created the Quickshare.
- Files** `strlist` `""`
- This preference states the file(s) that are provided via the Quickshare link. The setting reflects the content of the `Files` text field on the “Quickshare Administration” page.
- E-MailOnAccess** `bool` `FALSE`
- If this preference is set to `TRUE`, the creator of a Quickshare is notified by e-mail if a user opens a Quickshare. The setting reflects the state of the `E-Mail on Access` checkbox on the “Quickshare Administration” page.
- AllowDownload** `bool` `TRUE`
- If set to `TRUE`, this preference allows a Quickshare user to download files via Quickshare link. The setting reflects the state of the `Allow Download` checkbox on the “Quickshare Administration” page.
- AllowUpload** `bool` `FALSE`
- If set to `TRUE`, this preference allows a Quickshare user to upload files via Quickshare link. The setting reflects the state of the `Allow Upload` checkbox on the “Quickshare Administration” page.

AllowPreview `bool` `TRUE`

If set to `TRUE`, this preference allows a Quickshare user to preview files via Quickshare link. The setting reflects the state of the `AllowPreview` checkbox on the “Quickshare Administration” page.

Random `str` `""`

Specifies a random suffix string for the Quickshare URL (compare Fig. 4.4). This prevents clients from accessing Quickshares with empty passwords (see **QuickshareEmptyPassword** above) by simply entering Quickshare IDs.

8.5.4 Web Server preference keys HELIOS Admin needs to know

The following keys require a new login on HELIOS Admin Server to take effect:

Key: `Programs/websharesrv/websharewoa/<webserver>/<preference>`

When HELIOS Admin displays the “Quickshare” edit dialog, it includes information about the `Web Server` and `URL`.

If the WebShare File Server and Web Server are installed on different machines, HELIOS Admin needs to know the WebShare Web Server configuration for the following preference keys:

- `SSLPort`
- `WOHost`
- `WOPort`
- `WSAllowedHostNames`
- `WSHostName`
- `WSHostPort`
- `WSPublicHost`

For `<webserver>` in the preference key use the complete WebShare Web Server name or IP address, e.g.:

Example 1 (using the complete WebShare Web Server *name*):

```
mywebserver.domain.com
```

Example 2 (using the complete WebShare Web Server *IP address*):

```
172.16.3.29
```

If for example the WebShare Web Server has the changed SSLPort 4430, this would be the prefvalue call to set:

```
prefvalue -k "Programs/websharesrv/websharewoa/mywebserver.domain.com  
/SSLPort" -t int 4430
```

9 HELIOS Document Hub

HELIOS Document Hub allows access from iOS or Android devices to intranet file server volumes to present and use server documents online and offline. Built-in file synchronization ensures that server files are automatically updated on mobile devices. Enterprise file server security is enforced for online and offline use.

A user guide on how to use Document Hub is available in the app's help files.

10 WebShare security

10.1 Security considerations

10.1.1 WebShare Web Server

HELIOS WebShare's security is provided by a two-tier server application. The WebShare Web Server handles the web user interface on a separate server to ensure that the main file server is not accessible from the internet. In addition, SSL encryption is supported.

Port

Incoming HTTP port is 2009.

JavaScript

During the login process, the password is sent in encrypted form (RSA), as long as JavaScript is activated in the browser. If JavaScript is active, the browser will display `Crypted RSA 1024 bit` adjacent to the `Password` field (Fig. 6.2). If it is not, the word will be `cleartext` and the password is sent without any encryption to the WebShare server.

Note: With the `Enforce RSA Crypted Passwords` option in the "Server Preferences" window (see Fig. 4.3 in 4.1 "Server Preferences") encrypted user logins are enforced.

10.1.2 WebShare File Server

The server file system security will be enforced according to the user credentials. Sharepoint based security allows further restrictions per user, e.g. browse, preview, download, upload and file management.

Ports

Port 2010-2015

10.1.3 Server setup

We highly recommend to use a two-tier server setup which is comprised of a dedicated WebShare Web Server with two network adapters as illustrated in 3.1 “Different setups”. The benefit of this setup is:

- Only one HTTP port (default: 2009) is available from the internet
- HTTP traffic is handled on a dedicated server (HTTP attacks will not slow down the file server)
- The dedicated WebShare Web Server does not store any data (in case an unauthorized person is able to log in, they will not find any data)
- It is easier to secure the dedicated server with only one incoming TCP/IP port
- It is easier to use the latest OS updates on this dedicated server

10.1.4 Firewalls

We highly recommend to secure all TCP/IP ports of the WebShare Web Server and allow only incoming HTTP connections on port 2009 (WebShare HTTP

default). This can be done via a hardware firewall on an internet router or via a software firewall on the WebShare Web Server.

10.1.5 Access from the WebShare Web Server to the WebShare File Server

The WebShare Web Server preference **WSAllowedHostNames** (7.6 “Preferences”) allows limiting the WebShare Web Server access to a given list of WebShare File Servers. We recommend to specify the hosts which are allowed by the WebShare Web Server to avoid that an unauthorized person routes this HTTP traffic via your WebShare Web Server to their WebShare File Server. Though this is not a security problem, there should be no reason to allow others to use your WebShare Web Server.

10.1.6 Symbolic links within sharepoints

By default, WebShare hides all symbolic link files for security reasons. Irrespective of this, it can happen that a directory includes a symbolic link to some files outside of a sharepoint. When a user duplicates this directory, all references to symbolic links are resolved and copied into the duplicated directory. Therefore, the files will not be symbolic links anymore and can be accessed.

10.1.7 Action scripts

WebShare allows running custom scripts, which are stored in the “var/settings/WebShare/Actions” directory. All sample actions were developed as “Perl” scripts. “shell” or other programs are allowed but we recommend “Perl” to ensure server cross-platform compatibility, and avoid quoting problems of special characters in file names/arguments. Please note that action scripts

running with the host user ID (or equivalent permissions) can access data outside a sharepoint. For security reasons, you may want to control the action script availability to individual users by limiting the action script access permissions. This can be done using the file system permissions (UNIX “chmod” or Windows ACLs to set e.g. *access for user only*, *access for group only*). Action scripts calling host programs (via system, pipe open, shell, etc.) can be dangerous if the file names contain special characters (e.g. < or > or ‘). Consult an operating system or “Perl” scripting specialist to verify custom scripts.

10.1.8 Allow all Read or Read/Write access in sharepoints

The optional preference to bypass host permissions **AllRead** and **AllReadWrite** should not be used unless you are aware that the access to files is not protected by the host OS anymore. By default, these two preferences are turned off and can only be turned on via a special WebShare file preference.

10.1.9 “wsaddshare” and “wslogin” scripts

The optional “wsaddshare” script allows limiting the sharepoint administration to a few specific path names (e.g. only “/data” and “/webshare” are allowed). Set up a list of allowed path names via “wsaddshare” to ensure that the WebShare Administrator cannot publish the entire server.

The “wslogin” script allows additional auditing of user logins, e.g. verifying the remote address or limiting the login to specific hours/days.

10.1.10 No content security

By default, WebShare uses crypted passwords, nobody can spy these passwords because WebShare uses a random number which is different for each HTTP login. The complete content, e.g. file browsers, image previews and uploads/downloads, is sent over the internet without encryption in a default installation. internet providers, local users, etc. can use network monitoring tools to spy your activities. To avoid this, complete encryption via HTTPS can be enabled according to the instructions given in 7.4 “HTTP/SSL support”.

10.1.11 Switching WebShare to port 80 on the WebShare Web Server

This chapter provides more information about how to setup WebShare to use the default HTTP port and how to run WebShare in parallel with the existing web server on the same machine, using port 80 for the HTTP communication.

Some customers will not allow any other port than the default HTTP port 80. Changing the WebShare port to 80 offers more compatibility to other users behind their own proxy servers and firewalls.

By default WebShare accepts incoming HTTP connections from all IP addresses/network interfaces on port 2009. When the **WOPort** preference is changed to port 80 this may conflict with the existing web server (e.g. Apache) on the same host. The workaround is to setup a second IP address (alias) on the same interface and configure WebShare to use the second IP address on port 80. The DNS/Hosts configuration must be updated with the second IP address, e.g. “webshare.<yourdomain>.com” mapping to the second IP address. This can be done via:

```
# ifconfig eth0:0 192.168.1.6 up
```

This is the command for a Linux platform using the network interface “eth0” assigning the additional IP address. The command or syntax may vary on different server platforms, so check your options in the “ifconfig” or “ip” documentation. The IP address has to be valid within your internet network range/class.

The first step is to tell WebShare to listen only on the new interface instead of all interfaces.

- Specify the WebShare Web Server preference **WOHost**. The new name must resolve to the new alias IP address:

```
# prefvalue -k Programs/websharewoa/WOHost -t str  
"webshare.yourdomain.com"
```

- Then set the **WOPort** preference and then stop and restart the WebShare Web Server:

```
# prefvalue -k Programs/websharewoa/WOPort -t int 80  
  
# srvutil stop websharewoa  
# srvutil start websharewoa
```

A Special characters in file names

There are several characters in file/folder names which are handled specially when uploading or downloading. These are 9 characters, which have a special meaning for UNIX file names.

Even on Mac or Windows clients, not all of them can be used in file names.

Hexadecimal	Usual representation
22	"
2a	*
2f	/
3a	:
3c	<
3e	>
3f	?
5c	\
5e	^
7c	

When uploading a file with a name containing a character from this list, the file name stored in the server file system will not be represented with the original character. Instead, it is represented with a “^” followed by the hexadecimal encoding of the character. This encoding is also used by EtherShare.

For example, the file name “4*4 yields 16” will be stored as “4^2a4 yields 16” in the server file system. Similarly, when uploading a Zip archive containing a file or folder with a name containing a character from this list, the file name in the file system will contain the “^xy” representation.

When downloading a file with a name containing a quoted character from this list, it will NOT be translated to its unquoted form. Instead the representation will be the same. For example, a UNIX file name “4^2a4 yields 16” will be downloaded unchanged.

Similarly, when downloading multiple files, the Zip archive containing a file or folder with a name containing a quoted character from this list, the file name in the Zip archive will contain the “^xy” representation.

Note: The above mentioned escape rules for special characters are for internal handling only. In the GUI and in the file browser the WebShare Web Server will display the unescaped character.

B WOStarter – Web service health check

All HELIOS services are monitored by the HELIOS Service Controller. If a program aborts due to a major problem, the Service Controller will log errors and restart the service. The “wostarter.so” (WOStarter) is a plug-in for the Service Controller to constantly monitor its whole web service. If a web service gets stuck and is not responding correctly to HTTP requests from the WOStarter, the Service Controller will restart the service. This adds an additional level of availability auditing to the Service Controller.

The file “wostarter.so” is located in “HELIOSDIR/lib”. The HELIOS Service Controller can use this plug-in to start/stop and monitor the WebShare Web Server (“websharewoa”). It can be activated for the WebShare Web Server via the following preference:

```
# prefvalue -k 'Services/websharewoa/ServiceStarter' -t str  
"de.helios.servicestarter.wostarter"
```

WOStarter periodically checks whether the “websharewoa” service is still alive. WOStarter can detect the following web service failures:

- HTTP response does not contain an expected keyword
- HTTP response contains a keyword that is not expected
- HTTP error occurs
- HTTP response is incomplete
- No HTTP response at all

When WOSTarter detects a problem with its monitored web service, it will log detailed errors and restart the web service. Custom WOSTarter settings can be configured via preferences.

Examples:

The `WatchdogInterval` preference specifies the timeout in seconds (*default=600*):

```
# prefvalue -k 'Programs/websharewoa/WatchdogInterval' -t int [value]
```

The `WOHost` preference specifies the hostname or the IP address of the web service (*default=localhost*):

```
# prefvalue -k 'Programs/websharewoa/WOHost' -t str [value]
```

The `WOPort` preference specifies the port of the web service (*default=2009*):

```
# prefvalue -k 'Programs/websharewoa/WOPort' -t int [value]
```

The `ResponsePositive` preference specifies optional strings that must be contained in the HTTP response (*no default*).

```
# prefvalue -k 'Programs/websharewoa/ResponsePositive' -t strlist [value]
```

The `ResponseNegative` preference specifies optional strings that must be contained in the HTTP response and which indicate an error (*no default*).

```
# prefvalue -k 'Programs/websharewoa/ResponseNegative' -t strlist [value]
```

C Technical notes

C.1 WebShare log file structure

“HELIOSDIR/var/adm/webshare.acct” (with the appendices “.0”, *yesterday*, to “.6”, *seven days ago*) provides details for several WebShare actions.

The messages have the following format (from left to right):

```
date user ip action sharepoint path entry target user-agent result details
```

Description

date: Date and time in seconds since 1-1-1970 (UNIX “time_t” values)

user: Name of the logged-in user. The number of user logins per day is stated in parentheses. If a user has logged-in from HELIOS Admin, this is stated in the form *<user>(heladmin)*

ip: IP address of the logged-in client

action: Action that is taken, e.g. *login, preview, addShare*

sharepoint: Sharepoint where the action is taken

path: Path to file within the sharepoint

entry: File name in *download, upload, getFile* and *preview* action

target: File size in *download, upload, findFile, getFile* action, and used options in case of *preview* action

`user-agent`: In case of a *login* action, browser information (OS, browser, platform) is listed

`result`: Result *0* for success, *666* for failed login

`details`: File information in *download* and *upload* action

Index

A

Access keys	100
Accounting	41
Action scripts	
Calling action scripts via JavaScript	215
Examples	
wsannotations.pl	213
wscmdargs.pl	213
wsdialog.pl	213
wsdu.pl	213
wsimageinfo.pl	213
wslinks.pl	213
wsll.pl	214
wspdfinfo.pl	214
wssendmsg.pl	214
wsspotlightmeta.pl	214
wsxpvcollect.pl	214
wsxpvinfo.pl	214
Security	239
Add file comments	117
Administration	
Accounting	41
Branding Editor	44
Java Server Statistics	61
My User Preferences	142
Quickshare Administration	27
Server Preferences	21
Sharepoint Administration	35
User Administration	28

Annotations	130
B	
Branding Editor	44
Add custom banner images	55
Add custom file icons	55
Banner image URL mapping	55
Configuration file ("style")	54
Create and configure brandings	45
Custom actions icons	61
Custom toolbar icons	60
Customize brandings via CSS	57
Customize brandings via JavaScript	59
Import brandings	53
Browsers	
Supported browsers	147
C	
Certificates	
SSL	157
Characters	
Special characters in file names	243
Color Info	128
Comments	
Add file comments	117
Configuration	
HELIOS Admin	83
Custom icons (HELIOS Icon Collector)	68
Custom scripts	
wsaddshare.pl	209
wsemail.pl	210
wslogin.pl	208
Enhanced Document Hub security	209
wslogout.pl	210

Customization	
WebShare Web Server	155
D	
Debugging WebShare scripts	211
Document Hub	
Custom scripts	
wslogin.pl	209
Document previews	120
Drag & drop upload support	116
F	
File access permissions	118
File format support	146
File server	
Login	97
Preselect the WebShare File Server	98
Firewalls	
Security	238
H	
HELIOS Admin	
Configuration	83
Sharepoints (Lists menu)	88
WebShare Log Files (Lists menu)	95
WebShare Server Settings (Settings menu)	84
WebShare Users (Lists menu)	92
HELIOS Icon Collector	<i>see</i> WebShare utilities
Custom icons	68
Host user	23
HTTPS/SSL support	157
I	
Image Editor	124
Image previews	120

Installation	
Different setups	9
Hardware firewall (Internet)	11
Hardware firewall (Intranet)	11, 245
Single-server solution	12
Software firewall (Internet)	10
WebShare File Server	16
WebShare Web Server	13
J	
Java Server Statistics	61
JavaScript	
Calling action scripts via JavaScript	215
L	
Localization	
WebShare Web Server	155
Log files	
WebShare	247
Log in to WebShare	19
Log off from WebShare	119
Login	
File server login	97
Preselect the WebShare File Server	98
Logout	
File server logout	119
N	
Navigation	
Keyboard navigation for file browsing	102
New features in WebShare	6
O	
Optional scripts	
wspreviewaccess.pl	210

Organize sharepoints 34

P

Preferences

Quickshares

Active	231
AllowDownload	232
AllowPreview	233
AllowUpload	232
Comment	232
Creator	232
CreatorEMail	232
Expires	231
Files	232
Path	231
Random	233
Sharepoint	231
Username	231

Sharepoint

AllowAnnotations	228
AllowCopy	229
AllowDelete	229
AllowDownload	228
AllowPreview	228
AllowQuickshares	228
AllowRename	228
AllowUpload	228
AllRead	229
AllReadWrite	229
CollectMails	227
Comments	228
EmailAccess	227
EMailOnAccess	232
Groups	230
OnlyLayouts	229

*Preferences**Sharepoint (contin.)*

Path	227
Publish	227
Users	230
Web Server preferences keys HELIOS Admin needs to know	233
WebShare File Server	
AdminNotify	221
AliasPDF	227
AllowAllReadWrite	222
AllowEMailMessages	218
AllowForgotPassword	217
AllowHostUsers	221
AllowLinkShares	218
AllowQuickshares	218
AllowRegisterUser	217
AllowUserICCProfiles	222
AllowVirtualUsers	221
AnnotationPrefix	219
CacheDir	226
CacheSize	220
CustomPreviewTypes	224
DateFormat	222
DefaultMacintoshEncoding	223
DefaultWindowsEncoding	223
DisableUTCDelta	219
EnforceCryptedLogin	218
GlobalQuickshareUsers	218
HideSpecialFiles	223
ipaccess	226
logdenied	219
mail	223
MaxGalleryRes	220
maxuid	226
MaxUsersLimit	225

*Preferences**WebShare File Server (contin.)*

MaxWoaBlockSize	219
minuid	226
PreviewResolutions	223
ProofProfiles	222
QuickshareEmptyPassword	218
SendMailOnActionScript	223
sessionsPort	225
ShowHiddenFiles	223
TcpPort	225
TcpRecvSize	220
TcpSendSize	220
TelnetPort	225
URLImageOnlyUsers	224
URLSuffixSize	219
URLWebOnlyUsers	224
UserNotify	221
WrongAuthDelay	217

WebShare Web Server

JavaOptions	187
MDNSPort	180
SSLPort	180
WOHost	181
WOPort	180
WOSessionTimeOut	186
WSAllowedHostNames	185
WSDenyAccessForUA	182
WSDisabledSSLProtocols	183
WSDisableHTML5Upload	186
WSEventDisplayPassword	186
WSGZIPResponse	187
WSHostName	183
WSHostPort	185

*Preferences**WebShare Web Server (contin.)*

WSPrintJavaExceptions	187
WSPublicHost	182
WSRedirectToSSL	182
WSUpDownloadTimeOut	186
WSUploadChunkSize	186

WOStarter

ResponseNegative	188
ResponsePositive	187
WatchdogInterval	187

Previews

Documents	120
Images	120

Privileged transfer	29
---------------------------	----

Q

Quickshare Administration	27
---------------------------------	----

Quickshares

Create Quickshares	140
Using Quickshares	140

R

robots.txt	182
------------------	-----

S

Security

Action scripts	239
Firewalls	238
WebShare File Server	238
WebShare Web Server	237

Server Preferences	21
--------------------------	----

Server setup	238
--------------------	-----

Sharepoint

Work in a sharepoint	104
----------------------------	-----

Sharepoint Administration	35
Slideshow	106
Special characters in file names	243
SSL	
Certificates	157
Supported browsers	147
Symbolic links within sharepoints	239
T	
Telnet port	207
Troubleshooting	79
Limitations	82
U	
Upload	
Drag & drop upload support	116
Upload Zip files without automatic extraction	115
URL Share Access	68
URL Share Access Helper	75
User Administration	28
Utility programs	
unzipstream	196
wscommon.pm	200
wscopy.pl	201
wsdownload.pl	202
wsdup.pl	202
wsforgotpw.pl	204
wskeytool	162
wsmkdir.pl	202
wsmove.pl	201
wsmv.pl	203
wsperm.pl	206
wspreview.pl	203
wsregnewuser.pl	205
wsrm.pl	205

Utility programs (contin.)

wsupload.pl	206
wsuploadmv.pl	206
zipstream	194

V

Virtual user	23
--------------------	----

W

WebShare

Access keys	100
Log file	247
New features	6
URL Share Access	68
Work in a sharepoint	104

WebShare File Server

About	189
Installation	16
User configuration file	189
Utility programs	193

WebShare user

Host user	23
Virtual user	23

WebShare utilities

HELIOS Icon Collector	63
-----------------------------	----

WebShare Web Server

About	151
Customization/Localization	155
Installation	13
License information	151
Server files	152

Windows

Notes for WebShare users	30
--------------------------------	----

WOStarter – WebShare Health Check	245
---	-----