

Pier

Product Description and Functional Specification

Document ID	IM.PIER.INT.01
Document version	1.0
Date of issue	2026-10-06
Applies to	Pier 0.3.1
Language	English
Publisher	iMobile

Contents

- 1. General 3
 - 1.1. Name 3
 - 1.2. Purpose 3
 - 1.3. Field of use 3
 - 1.4. Type of software 3
- 2. Functions 3
 - 2.1. Mounting storage as drives 3
 - 2.2. Local cache 4
 - 2.3. Write-back, resume and reconnection 4
 - 2.4. Offline mode 5
 - 2.5. Server check and name validation 5
 - 2.6. Pier Backup 5
 - 2.7. Managing the product 5
 - 2.8. Updating 6
- 3. Architecture and components 6
 - 3.1. Components 6
 - 3.2. Where data is kept 6
- 4. Interfaces and data exchange 6
 - 4.1. Storage protocols 6
 - 4.2. Exchange with the vendor's account server 7
 - 4.3. Local interfaces and formats 7
 - 4.4. Cryptography 7
- 5. Editions and limitations 7
 - 5.1. Editions 7
 - 5.2. Registration 8
 - 5.3. Known limitations 8
- 6. Environment requirements 9

About this document

This document describes what Pier version 0.3.1 does: its purpose, functions, components and architecture, the protocols and formats it uses, its editions and its known limitations.

It is written for the customer's specialists who evaluate the product and for reviewers who check the stated characteristics. Installation and configuration are covered in the Installation and Administration Guide, and day-to-day use in the User Guide.

1. General

1.1. Name

The product is called Pier. This document covers version 0.3.1, released on 4 October 2026. The vendor is iMobile. The product includes the backup tool Pier Backup.

1.2. Purpose

Pier mounts remote file storage as Windows drive letters. It supports WebDAV (including Nextcloud and ownCloud servers), SFTP and NFS version 3. File Explorer and other programs use a mounted drive the same way they use a local disk.

Pier Backup makes versioned, encrypted backups of folders on the computer to WebDAV, SFTP, NFS and S3 storage and restores files from them.

1.3. Field of use

Windows workstations and servers that need to work with files on remote storage as if they were local, including over slow or unreliable links and with large files.

1.4. Type of software

A system utility for Windows: a network storage client with a built-in backup tool. It is installed on the computer where the drives are used. There is no server component on the customer side and no data storage on the vendor side.

2. Functions

2.1. Mounting storage as drives

Each drive is defined by a protocol, a server address, a path on the server, credentials and a drive letter from D to Z. Drives are mounted by a Windows service, so a drive:

- is visible to every user of the computer in every session;
- is mounted when the service starts, without anyone signing in, if "Mount at start" is selected;
- can be mounted read-only (the "Read only" option).

What a drive can do depends on the protocol and the server.

Capability	WebDAV	SFTP	NFS version 3
Reading part of a file	yes, if the server honours Range requests	yes	yes

Capability	WebDAV	SFTP	NFS version 3
Writing at an arbitrary offset	no, a changed file is sent whole	yes	yes
Resuming an interrupted upload	Nextcloud and ownCloud: by chunks; other servers: from the start of the file	yes	yes
Resuming an interrupted download	yes, if the server honours Range requests	yes	yes
Passing the file modification time	if the server allows it (Nextcloud, ownCloud)	yes	yes
Free space information	if the server reports a quota	if the server supports the statvfs extension	yes
Authentication	login and password (Basic; Negotiate, NTLM or Digest when the server demands it)	password or SSH key	uid and gid values (AUTH_SYS)
Channel protection	TLS (HTTPS)	SSH	none

S3 storage cannot be mounted as a drive; it is used for backups only.

2.2. Local cache

File content is read from the server in blocks and kept in a cache on the local disk. Only the blocks that programs actually read are downloaded, each of them once. The following can be set per drive:

- block size, from 64 KB to 16 MB (1 MB by default);
- maximum cache size, 4096 MB by default and at least 64 MB; by default data not yet sent to the server is never evicted;
- read-ahead for sequential access, from 4 to 32 blocks by default;
- how long file and folder information is trusted, 10 seconds by default;
- the size below which a file is fetched whole when it is opened, 4 MB by default.

Files on a server that ignores Range requests are read as one sequential stream.

2.3. Write-back, resume and reconnection

Writes go to the cache; the upload to the server starts in the background after the file is closed (2 seconds later by default). The upload queue is kept on disk and survives a service restart, a reboot and a loss of connection.

An interrupted download continues from the first missing block. An interrupted upload continues from the last confirmed offset (SFTP, NFS) or from the last accepted chunk (Nextcloud, ownCloud). After an upload the product compares the file size on the server.

After a network error an operation is retried with a growing delay (by default up to 5 attempts, 0.5 to 30 seconds apart); uploads are retried until they succeed by default. The service watches for network interface changes and for the computer waking from sleep and reconnects.

Timeouts, the number of connections (4 by default, at most 32), the upload chunk size (16 MB by default), the number of chunks of one file sent in parallel (2 by default, at most 16) and a speed limit can be set per drive. Running and queued transfers are listed on the Transfers tab. An upload can be stopped; the local changes to that file are then dropped.

2.4. Offline mode

A drive can be switched to offline mode (the Offline button): reads are served from the cache only, and changes are queued and sent to the server when the drive goes back online. A block that is not in the cache cannot be read in offline mode.

2.5. Server check and name validation

Before a new drive is saved, and when Check is pressed, the product connects to the server and, in a temporary folder `.pier-probe-<random value>` in the root of the mounted folder, tests writing and reading a file, reading part of a file, writing at an offset, setting the modification time, renaming over an existing file, case sensitivity of names, 255-byte names and Unicode names. The folder is then removed. The result is shown as a report, stored with the drive and determines how the product works with that server. A new drive is saved only if the connection to the server succeeds.

When files are created or renamed, the product refuses, before contacting the server, names that the server or Windows cannot hold: Windows reserved names, names ending in a dot or a space, names longer than the server allows, and names that differ from an existing one only by letter case (on case-sensitive servers). The rules are set on the Compatibility page.

2.6. Pier Backup

A backup job consists of source folders, masks of files to skip, the destination (a folder on the server of a drive that is already configured, or a separate WebDAV, SFTP, NFS or S3 server), a backup password, a schedule and retention rules.

- Every run creates a version: a snapshot of all the folders of the job. A file whose size and modification time have not changed is not read. A changed file is split into content-defined blocks (512 KB to 8 MB), and only blocks the server does not yet hold are sent.
- Data is compressed (compression can be turned off per job) and encrypted on the computer before it is sent. The server holds only the encrypted files of the backup repository; file names and the folder structure are not visible to it. The backup password cannot be recovered.
- Any version can be restored as a whole, as one folder or as one file, to its original place or to another folder. Files that already match the version are not downloaded again. Content, modification time and file attributes are restored.
- An interrupted run does not start over: the next run sends what is missing. A scheduled run that failed is retried after 30 minutes, at most five times.
- Retention rules set how many latest, daily, weekly and monthly versions are kept (10, 7, 4 and 12 by default). The space of deleted versions is reclaimed at most once a week, or on command.
- Verifying a copy downloads every repository file, checks its checksum and decrypts every block.
- Schedule (Pro edition): every few hours, or daily at a set time.
- Jobs run one at a time. Only members of the local Administrators group can configure and start backups.

2.7. Managing the product

- A notification-area icon: drive status, mounting and unmounting, opening a drive in File Explorer, immediate synchronisation, update control.
- A settings window with the tabs Drives, Backup, Transfers, Log, Account and Settings.
- The `Pier.exe` command line for scripts and for computers without a desktop: status, drive management, server check, backup and restore, update.

- The interface is available in 16 languages. Error messages of the service, command-line output and logs are in English.

2.8. Updating

Every 6 hours the service asks the vendor's account server whether a new version exists, verifies the signature of the reply, downloads the file and checks its SHA-256 checksum. With auto-update on, the new version is installed when no transfer or backup is running. Auto-update can be turned off in the icon's menu or on the Settings tab.

3. Architecture and components

3.1. Components

The product is a single executable, `Pier.exe`, which runs in several modes, and it relies on the Dokany driver.

Component	Role
Windows service "Pier"	Runs as LocalSystem and starts automatically (delayed start). Mounts the drives, maintains the cache and the upload queue, runs backups and checks for updates
Icon and settings window	Run in the user's session and talk to the service. They perform the registration with the vendor's account server
Command line	The same operations for scripts
Dokany driver 2.3.1	A third-party user-mode file-system driver (the <code>dokan2.dll</code> library under LGPL 3, the driver under the MIT licence). Installed as a separate package by the setup program

Inside the service a file-system request passes through the driver adapter, the volume (file operations), the cache (file information, data blocks, journal of pending uploads) and the protocol module (WebDAV, SFTP, NFS, S3). The settings window and the command line exchange JSON messages with the service over a local named pipe, `\\.\pipe\Pier`; connections to the pipe from other computers are rejected. The product opens no inbound network ports.

3.2. Where data is kept

Data	Location
Settings and drives	<code>%ProgramData%\Pier\config.json</code> ; passwords and keys under DPAPI protection
Cache and upload queue	<code>%ProgramData%\Pier\cache</code> , one folder per drive (configurable)
Backup jobs	<code>%ProgramData%\Pier\backup</code> ; accessible to SYSTEM and administrators only
Logs	<code>%ProgramData%\Pier\service.log</code> , <code>%LOCALAPPDATA%\Pier\tray.log</code>
Account information	<code>%LOCALAPPDATA%\Pier\account.json</code>

4. Interfaces and data exchange

4.1. Storage protocols

Protocol	Implementation
WebDAV	HTTP and HTTPS provided by Windows (WinHTTP) with automatic proxy discovery. Methods PROPFIND, GET (also with Range), PUT, MKCOL, MOVE, DELETE, PROPPATCH; chunked upload by the Nextcloud protocol
SFTP	SSH-2 and SFTP through the libssh2 1.11.1 library; the OpenSSH extensions posix-rename and statvfs
NFS	The product's own NFS version 3 client over TCP (ONC RPC, XDR, the MOUNT protocol, the portmapper service). The Windows "Client for NFS" feature is not needed
S3	The REST interface through WinHTTP: AWS Signature Version 4, ListObjectsV2, GET with Range, PUT, multipart upload, copying and deleting objects

4.2. Exchange with the vendor's account server

The product contacts the vendor's account server, `accounts.new-imobile.com`, over HTTPS with JSON requests: registration by e-mail address, fetching the edition terms, checking for and downloading updates and, in the Free edition, fetching ads and reporting that they were shown. The Dokany driver installer is downloaded from the vendor's website when it is needed. File content and names, storage addresses and credentials are not sent to the vendor. There is no telemetry and no crash reporting. The exact data sent is listed in the Installation and Administration Guide.

4.3. Local interfaces and formats

There is no programming interface (API) for third-party software other than the command line. Drives and backup jobs can be defined with JSON files. Backups are kept in the product's own format (a `pier-backup` repository, version 1) and can be read only by Pier.

4.4. Cryptography

- WebDAV and S3: TLS provided by Windows (Schannel); the product enables TLS 1.2 and 1.3. The server certificate is validated against the Windows certificate store; validation can be switched off in the drive settings.
- SFTP: the algorithms of the libssh2 1.11.1 library, with Windows CNG performing the cryptographic operations. Key exchange uses ECDH on the NIST P-256, P-384 and P-521 curves and Diffie-Hellman; ciphers are ChaCha20-Poly1305 and AES in CTR and CBC modes, plus 3DES-CBC and RC4 for compatibility with old servers; server host keys are ECDSA and RSA. The user authenticates with a password or with an RSA, ECDSA or Ed25519 key.
- Backups: AES-256-GCM; the key is derived from the backup password with PBKDF2-HMAC-SHA256 (600,000 iterations); block identifiers are HMAC-SHA256 values.
- Passwords and keys in the configuration: Windows DPAPI.
- Edition terms and update information: an ECDSA P-256 signature verified with a built-in public key.
- NFS: no encryption. The cache on the local disk is not encrypted.

The complete list of algorithms by name is given in the Security and Data Protection Statement, section "Cryptography".

5. Editions and limitations

5.1. Editions

Characteristic	Free	Pro
Drives mounted at once	up to 5	unlimited
Protocols, cache, resume, offline mode, running as a service, auto-update	yes	yes
Backup jobs	1	unlimited
Starting a backup	by hand	by hand and on a schedule
Restore, browsing versions, verifying a copy	yes	yes
Ads: a banner in the settings window and an ad pop-up at most once a day	yes, after registration; the date ads start is shown on the Account tab	no
Computers per e-mail address	up to 3	up to 10

The Pro edition is a one-year subscription; it is taken out in the iMobile account and bound to an e-mail address. When the subscription ends, backup jobs are kept and can be started by hand; restoring is never restricted.

5.2. Registration

For the first 14 days after its first start the product works without registration. After that, mounted drives, transfers and restoring from backups keep working, while adding or changing drives and creating, changing or starting backup jobs require the free registration by e-mail address. Registration needs access to the vendor's account server; there is no registration without Internet access.

5.3. Known limitations

- 64-bit (x64) Windows only; the Dokany driver is required.
- S3 is used for backups only. NFS is limited to version 3 over TCP with AUTH_SYS authentication and no encryption; symbolic links are shown as empty files.
- SFTP: the server's host key is neither verified nor remembered, so there is no protection against an impersonated server. Ed25519 host keys and Curve25519 key exchange are not supported. Keys in PuTTY (.ppk) format must be converted to OpenSSH format.
- WebDAV on servers other than Nextcloud and ownCloud: a changed file is sent whole and an interrupted upload starts over. TLS client certificates are not supported.
- There is no file locking and no merging of versions: when a file has been changed both on the computer and on the server, the local version is sent to the server.
- A mounted drive is available to every user of the computer with the rights of one server account.
- Changes not yet sent to the server exist only in the computer's cache and are lost when the drive is removed.
- Pier Backup does not use the Volume Shadow Copy Service (VSS): a file that another program holds open without read sharing is left out of the version. Cloud-only files and folder links are skipped. NTFS permissions and alternate data streams are not saved. The backup password cannot be changed.
- Pier Backup with S3 was verified against an S3-compatible server; it has not been verified against Amazon S3 or MinIO.
- The executable and the setup packages of version 0.3.1 carry no code-signing signature.
- There is no central management (Group Policy, administration console) and no record of user actions.

6. Environment requirements

- Windows 10 version 1809 or later, Windows 11, or Windows Server 2019 or later; 64-bit (x64) only.
- The Dokany driver 2.3.1 (installed by the product's setup program).
- Administrator rights for installation.
- Local disk space for the cache.
- Network access to the storage servers; Internet access to the vendor's account server for registration and updates.

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	0.3.1	First issue