

Pier

Security and Data Protection Statement

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

Contents

- 1. Deployment model 3
- 2. Data processed 3
 - 2.1. Personal data 3
 - 2.2. Where data is stored 3
 - 2.3. Data sent to the vendor 4
- 3. Access control 4
- 4. Cryptography 4
- 5. Logging and audit 5
- 6. Data export and deletion 5
- 7. Updates and vulnerability handling 6
- 8. Certifications and assessments 6
- 9. Accessibility 6
- 10. Known limitations 6

About this document

This statement describes how Pier version 0.3.1 handles data and which security mechanisms it implements. It describes the product as shipped. It is not a certification and does not replace the customer's own risk assessment.

1. Deployment model

Desktop software installed on the customer's computers.

The product is installed on every Windows computer (workstation or server) that needs the drives. It is a single executable, `Pier.exe`, which runs as the Windows service "Pier" (LocalSystem account), as a notification-area icon with a settings window in the user's session, and as a command-line program. Drives are presented through the Dokany file-system driver, installed as a separate package by the product's setup program. There is no server component on the customer side and no storage on the vendor side: the product talks to the storage servers the customer configures and to the vendor's account server (registration, edition terms, updates).

When installed on the customer's equipment, the product runs on infrastructure the customer controls, and the vendor has no access to the content processed there. Connections the product makes to third-party services that the customer configures are described in the Product Description.

Independently of the deployment option, the vendor receives the data listed under "Data sent to the vendor".

2. Data processed

2.1. Personal data

- The e-mail address of the person who registers the product (sent to the vendor's account server)
- A computer identifier computed as a hash of the Windows MachineGuid, and the computer's network address as seen by the vendor's server when it is contacted
- Credentials for the customer's storage servers: logins, passwords, SSH private keys, S3 access keys (stored on the customer's computer only)
- The content and names of files on mounted drives and in backups, which is whatever the customer keeps there, personal data included (processed on the customer's computer and sent only to the storage servers the customer configures)
- Server names, logins and file paths in the product's local logs

2.2. Where data is stored

The product's data is kept on the customer's computer. In `%ProgramData%\Pier:` the file `config.json` with the settings and drives (passwords and keys under DPAPI protection), the folder `cache` with the block cache of files and the queue of unsent changes (the cache location is configurable), the folder `backup` with the backup jobs, the state of the last run and the job logs (accessible to SYSTEM and administrators only), the files `install.json` (date of the first start) and `license.json` (signed edition terms), the folder `update` with downloaded update files, and the logs `service.log`, `update.log` and `setup.log`. In the user's `%LOCALAPPDATA%\Pier:` the file `account.json` (e-mail address, account token under DPAPI protection, edition terms), the folder `ads` (ad pictures) and the log `tray.log`. Files of mounted drives and backups are kept on the servers the customer configures. File content and names, storage addresses, logins, passwords and keys are not sent to the vendor. The product has no telemetry and no crash reporting.

2.3. Data sent to the vendor

- Request for a registration code: e-mail address, product identifier, interface language
- Activation: e-mail address, the code from the e-mail, product identifier, computer identifier
- Fetching the edition terms when the product's icon starts, once an hour while it runs and on the Refresh license button: account token, product identifier, product version, interface language, computer identifier
- Update check by the service 90 seconds after it starts, every 6 hours and on command: product identifier and product version, followed by the download of the new version's file when there is one
- In the Free edition when ads are shown: download of the ad pictures, and reports that an ad was shown or clicked (token, product identifier, event type, ad identifier)
- Download of the Dokany driver installer from the vendor's website when the driver is missing and the user agreed to install it, or when an update being installed needs it

3. Access control

The product has no user accounts or sign-in of its own. It accesses a storage server as the server account set in the drive's configuration (login and password, SSH key, uid and gid values for NFS, S3 access keys); the product performs no multi-factor authentication. A mounted drive is available to every user of the computer with full rights at the Windows level, while the rights on the server are those of the account configured for the drive. Any user signed in on the computer can add, change, mount and remove drives: the service's local control channel is open to authenticated users, and connections to it from other computers are rejected. The service performs backup operations only for members of the local Administrators group; a restore writes files with the rights of the user who requested it. Installation and removal require administrator rights. The account with the vendor is confirmed by a one-time code sent by e-mail.

4. Cryptography

- WebDAV and S3 channels: HTTPS provided by Windows (WinHTTP, Schannel). The product enables TLS 1.2 and TLS 1.3, and the actual version and cipher suite are decided by the operating system and the server. The server certificate is validated against the Windows certificate store, and validation can be switched off in the drive settings. Plain HTTP without encryption is possible when the user configures it
- WebDAV authentication: HTTP Basic (login and password in the request header) or, when the server demands it, Negotiate, NTLM or Digest through WinHTTP. S3 requests are signed with AWS Signature Version 4 (HMAC-SHA256, SHA-256 payload hash)
- SFTP channel: the SSH-2 protocol, the libssh2 1.11.1 library with Windows CNG for cryptographic operations. Key exchange: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1. Host keys: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256, ssh-rsa. Ciphers: chacha20-poly1305@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour, 3des-cbc. MACs: hmac-sha2-256, hmac-sha2-512 (also in encrypt-then-MAC mode), hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96. Algorithms are chosen by negotiation with the server. The product does not verify or remember the server's host key
- SFTP authentication: password, keyboard-interactive, or the user's private key of type RSA, ECDSA (nistp256, nistp384, nistp521) or Ed25519. Ed25519 signatures are made by built-in code derived from TweetNaCl, RSA and ECDSA signatures by Windows CNG. OpenSSH-format keys protected by a

passphrase are decrypted with bcrypt-pbkdf and AES-256-CTR

- NFS version 3: no encryption and no cryptographic authentication (AUTH_SYS)
- Pier Backup copies are encrypted on the computer before they are sent: AES-256-GCM (Windows CNG), a random 96-bit nonce per block, a 128-bit authentication tag. The 256-bit encryption key and the 256-bit identifier key are produced by the Windows random number generator and written to the backup repository encrypted under a key derived from the backup password with PBKDF2-HMAC-SHA256 (600,000 iterations, 256-bit salt). Block identifiers are HMAC-SHA256 values, and repository file names are the SHA-256 of their content
- Secrets on the computer: passwords and private keys of drives and backup jobs are protected with Windows DPAPI bound to the computer, the account token with DPAPI bound to the Windows user. The block cache of files on the local disk is not encrypted
- Exchange with the vendor's account server: HTTPS provided by Windows (WinHTTP, Schannel), TLS versions as configured in the operating system. Edition terms and update information are signed with ECDSA P-256 and SHA-256 and verified with a built-in public key. The update file and the driver installer are checked by SHA-256

5. Logging and audit

The service keeps a text log, `%ProgramData%\Pier\service.log`: start and stop, results of server checks, mounts, errors, file uploads with their paths, update checks and edition terms. At 4 MB the file is renamed to `service.log.1` and the previous `service.log.1` is deleted. Separate logs: `update.log` and `setup.log` in the same folder, `tray.log` in `%LOCALAPPDATA%\Pier`, and a `log.txt` for each backup job under `%ProgramData%\Pier\backup` (up to 1 MB, after which the older half is dropped). There is no record of user actions that says who performed an operation. The product does not write to the Windows event log and does not forward logs to external systems.

6. Data export and deletion

Files on mounted drives remain ordinary files on the customer's servers and can be reached with any client of the same protocol, without Pier. Backups are kept in the product's own format and can be read only by Pier with the backup password; data is taken out of them by restoring the required version to a folder. Settings are kept in JSON files. Removing a drive in the settings window deletes its cache together with any unsent changes. Backup versions are deleted in the restore window or with the commands `Pier.exe backup forget` and `Pier.exe backup prune`, and a whole backup by deleting its folder on the server. After the product is uninstalled, the folders `%ProgramData%\Pier` and `%LOCALAPPDATA%\Pier` are deleted by hand. The product has no function for deleting the registration data held by the vendor's account server.

7. Updates and vulnerability handling

Ninety seconds after it starts and then every 6 hours, the product's service asks the vendor's account server for the latest version, sending the product identifier and the installed version number. The reply is signed with an ECDSA P-256 key; the product verifies the signature, downloads the new executable and checks its size and SHA-256 checksum. With auto-update on (the default) the file is installed when no transfer or backup is running: the service stops, the executable is replaced and the service starts again, and the drives are unavailable meanwhile (about a minute). With auto-update off the product only announces the new version and the user starts the installation from the icon's menu, from the Settings tab or with the command `Pier.exe update apply`. The product can also be updated by running the setup package of the new version over the installed one; settings, drives and the cache are kept. The product has no built-in way to return to the previous version.

Suspected vulnerabilities can be reported through:

- contact form: <https://new-imobile.com/contact>
- e-mail: admin@new-imobile.com

Reports are handled as described in the document "Software Lifecycle, Maintenance and Support".

8. Certifications and assessments

No third-party security certification or audit (for example Common Criteria, FIPS 140-3, ISO/IEC 27001 or SOC 2) is claimed for the product or for the vendor in this document.

9. Accessibility

No accessibility conformance assessment has been carried out. The interface is built from standard Windows controls: controls can be reached from the keyboard and are exposed through UI Automation (the automated interface tests rely on this), windows scale with the display settings (Per-Monitor DPI v2), and right-to-left layout is used for Arabic and Persian.

10. Known limitations

- The product runs only on 64-bit (x64) Windows and needs the Dokany 2.x driver; without the driver no drive can be mounted
- S3 storage is used only as a place for backups; it cannot be mounted as a drive
- NFS: version 3 over TCP with AUTH_SYS authentication only, without encryption and without Kerberos; NFS version 4 is not supported; symbolic links are shown as empty files and special files are not shown
- 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. SSH agents, proxies and jump hosts are not supported. Keys in PuTTY (.ppk) format and EC keys in PEM format must be converted to OpenSSH format
- WebDAV: on servers other than Nextcloud and ownCloud any change to a file re-sends the whole file, and an interrupted upload starts over. TLS client certificates are not supported. WebDAV locks (LOCK) are not used
- 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; there is no separation by Windows user on the drive

- The cache on the local disk is not encrypted. Changes not yet sent to the server exist only in this computer's cache and are lost when the drive or the cache folder is deleted
- After 14 days without registration, drives and backup jobs cannot be added or changed and backups cannot be started. Registration needs access to the vendor's account server over the Internet
- 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 (OneDrive placeholders and the like) and folder links are skipped. NTFS permissions and alternate data streams are not saved
- Pier Backup: the backup password cannot be changed. Days of the week in a schedule can be set only in the job file. The backup repository has its own format. S3 was verified against an S3-compatible server and 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, so Windows may show an unknown-publisher warning
- There is no central management (Group Policy, administration console); configuration is done on each computer and automated through the command line
- There is no record of user actions. The product does not write to the Windows event log
- The product's notification-area icon does not start automatically when a user signs in; the drives do not depend on it
- Error messages of the service, command-line output and logs are in English only

Document history

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