Storage

Applies to userXpress 2.0.0.0

Find user settings and working files, protect saved logons and understand passphrase reset and cache clearing.

Storage locations

- **Profile and logs:** `%APPDATA%\Delorion\UserXpress` contains settings, saved connections, queries and application logs. Startup diagnostic reports are stored under its `Diagnostics\Startup` subfolder.
- **Cached system metadata:** encrypted cache files are stored in `%LOCALAPPDATA%\Delorion\UserXpress\EncryptedCache`.
- **Workbooks, exports and reports:** these are in the folders selected when opening or saving files, which can be outside the application-data folders.

To open a default location, paste the path into File Explorer's address bar in the intended user's Windows session. `%APPDATA%` and `%LOCALAPPDATA%` resolve to that user's profile.

Protect credentials and working files

The local userXpress passphrase unlocks saved SAP logon credentials. The application decrypts them when it opens the saved connection.

A workbook can contain new-user passwords. A report can contain user IDs, names and role assignments. Use Excel export protection to require a password when opening an exported Excel file.

Store exports and logs in locations approved for their contents and restrict access accordingly.

SAP connection credentials

Saved logons and Auto Start entries use **AES-256-GCM**. A randomly generated 256-bit key encrypts the saved SAP user IDs and passwords. GCM provides encryption and tamper detection together.

The local passphrase protects this credential-encryption key through **Argon2id**:

Parameter	Value
Algorithm	Argon2id, version 1.3
Memory	256 MiB
Passes	3

Parameter	Value
Parallelism	4 lanes
Salt	32 random bytes
Derived key	256 bits

The derived key encrypts the credential-encryption key using AES-256-GCM. Each encryption uses a fresh random 12-byte nonce and a 128-bit authentication tag. A nonce is the per-encryption value used by GCM, and the tag detects changes to the protected data.

Authentication binds each saved credential to its profile, SAP system, client and field. The credential file's connection definitions and protected key are also authenticated. userXpress checks this protection before using the saved credentials.

userXpress session password

The session password is the local passphrase entered when starting or unlocking userXpress.

userXpress verifies the passphrase by deriving the Argon2id key and using it to authenticate and unlock the credential-encryption key. The same mechanism verifies the passphrase and protects saved logons. There is no separate password hash in this profile format.

Argon2id runs during unlock. userXpress then reuses the unlocked credential key when reading or saving logons, rather than repeating key derivation for each SAP user ID or password.

Changing the passphrase protects the same credential key with the new passphrase. Saved logons and connection definitions remain available. Resetting a forgotten passphrase creates a new key and clears the saved logons, as described in Reset a forgotten passphrase.

Excel export protection

Excel exports can be encrypted with a password that the recipient must enter to open the file. Protection is off by default. Enable **Protect Excel exports** in **Settings** and enter a **Default Excel password**. For automatic protection and per-export choices, see Excel export settings.

The default Excel password is stored in your userXpress profile, encrypted with **AES-256-GCM**.

Exported workbooks use Excel's password-to-open encryption. Recipients enter the password used for that file. You can use the saved default or choose a different password for one export. Choosing a password for one file leaves the saved default unchanged.

Changing the userXpress passphrase preserves the saved default Excel password. Resetting a forgotten passphrase clears that default. Previously exported files still require the password used when they were created, so retain that password for as long as the files are needed.

This option protects Excel workbooks. CSV, XML, logs and other output formats retain their own storage and access requirements.

Cached metadata

userXpress caches SAP function and table definitions, authorization objects, transaction codes and related lookup values. It also stores table counts and previous loading times to help prepare subsequent loads.

These files can reveal technical information about your SAP landscape, so keep the cache within the administrator's protected Windows profile.

Persistent cache files have three protections:

- **Encryption:** AES-256-CBC with PKCS#7 padding and a random initialization vector.
- **Tamper detection:** HMAC-SHA256 checks the authenticated file contents before decryption.
- **Key protection:** Windows Data Protection API (DPAPI) protects encryption and authentication keys for the current Windows user.

Copying the cache to another account does not provide that account with usable SAP metadata. If a cache entry cannot be authenticated or decrypted, userXpress ignores it and requests the information from SAP again.

Cache protection does not encrypt logs, exports or account-creation workbooks.

Reset a forgotten passphrase

A reset clears saved SAP user IDs, SAP passwords and the default Excel password. It also turns off AutoStart for the affected entries. Connection definitions, favorite selections and language settings remain available. It does not reset any SAP user's password. Make sure the administrator can obtain their SAP logon details again before proceeding.

1. At the userXpress unlock window, choose **Reset...**.
2. Read the warning and confirm only if you are prepared to re-enter the saved logons.
3. Enter and confirm a new passphrase in **New Passphrase**, then choose **OK**.
4. Re-enter the SAP credentials for the affected connections and verify them before enabling AutoStart again.
5. Set **Default Excel password** again before using automatic Excel export protection. Previously exported files retain the password used to create them.

If the current passphrase is still known, choose **Session Password** on the main toolbar to change it. Reset is the recovery path for a forgotten passphrase.

Back up user configuration

1. Finish active SAP operations and close userXpress.
2. Copy the user's settings directory to a protected backup location. Record the application version and the Windows account the backup belongs to.

3. Preserve any account-creation or recovery workbook still needed for unfinished work. Include exports only where your retention policy requires them.

Keep the passphrase available to the account owner. Do not use one person’s configuration backup as a template for other administrators: it can contain saved SAP credentials and personal settings.

Clear cached data

Use **Information** → **Diagnostics** → **Clear cache…** to remove stored cache files when troubleshooting cached information or retiring a workstation. Read the confirmation and choose **OK**.

The result reports the number of files removed. An error can mean the cache was only partly cleared.

Cache clearing removes stored cache files. It does not remove saved queries, all settings, exports or workbooks. The next operation can take longer while information is read from SAP again.

Persistent encrypted cache files are checked for corruption before use, and their keys are protected for the current Windows user. Cached metadata and value suggestions help the application prepare SAP requests. They are not a saved list of matching roles.

Run the role content filter again when you need updated results.

Retention and removal

Retain bulk-operation recovery files until the operation has been reconciled. Then remove files containing credentials or personal data according to your retention policy. Apply that policy to backups and shared export folders as well as the local workstation.

When removing userXpress, review the settings folder, cache, diagnostic reports and user-selected output folders separately from uninstalling the program.

Before sharing any of those files with support, follow Review files before sending.