userXpress documentation

userXpress Technical Documentation

Document Information

Field	Value
Document Title	userXpress Technical Documentation
Document Version	1.0
Publication Date	October 26, 2026
Applicable Software Version	userXpress 2.0.0.0
Document Owner	Delorion B.V.
Classification	Customer Documentation
Status	Final

© 2026 Delorion B.V. All rights reserved.

Contents

Technical Documentation

- Architecture
- System requirements and compatibility
- Audit
- Storage

© 2026 Delorion B.V. All rights reserved.

Architecture

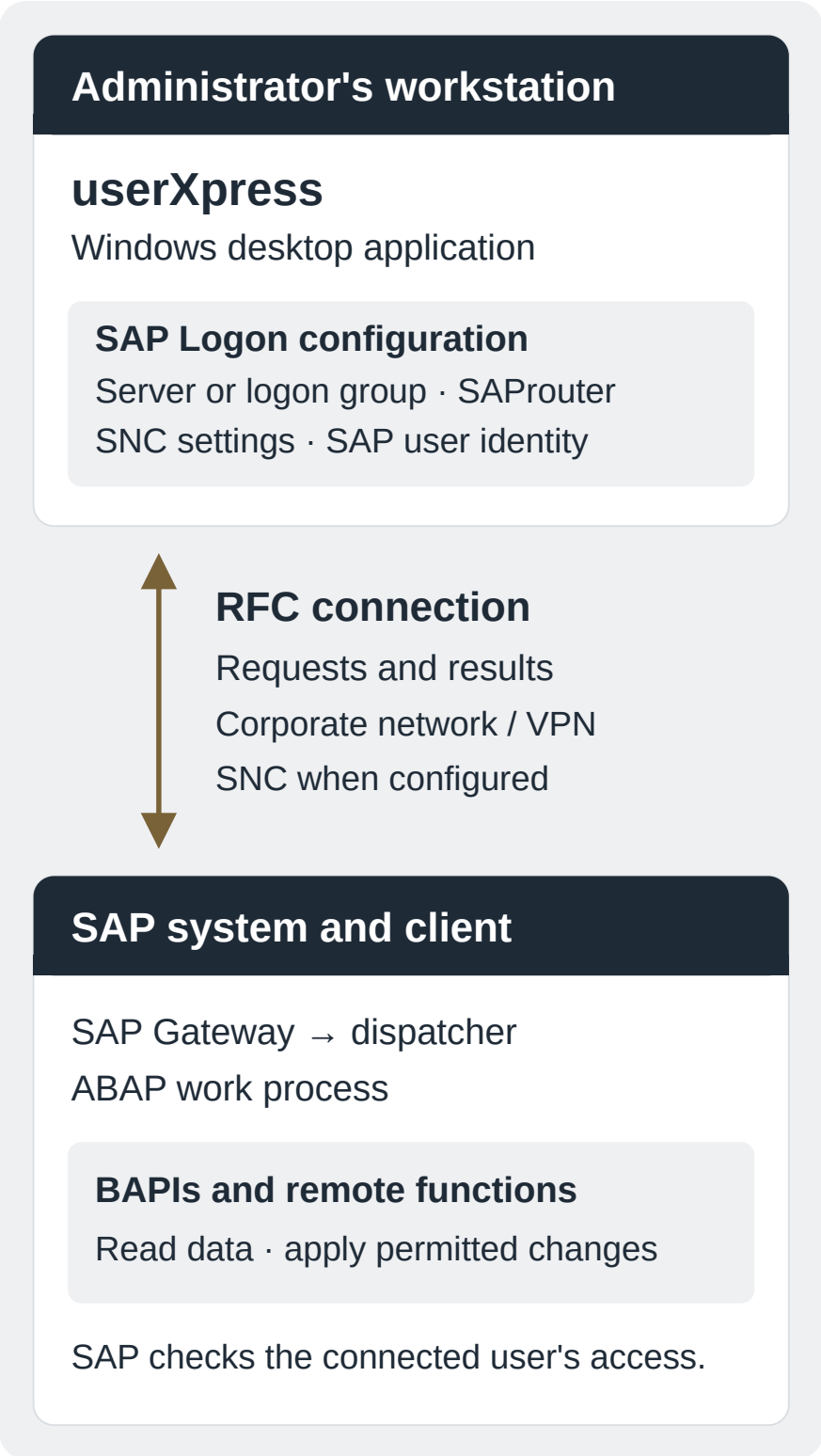
Applies to userXpress 2.0.0.0

Understand how userXpress connects to SAP, authenticates administrators and reads or changes SAP data.

userXpress runs on the administrator's Windows workstation and communicates directly with the selected SAP systems.

It uses the connection definitions maintained for SAP Logon: application server or logon group, system number, SAProuter route and SNC settings. No intermediary userXpress server is required for these SAP connections.

© 2026 Delorion B.V. All rights reserved.



How userXpress connects to SAP

A remote function call (RFC) lets userXpress request an operation on the SAP system. SAP checks the connected user’s authorizations, executes the function and returns data or a result.

Many account operations use SAP Business Application Programming Interfaces (BAPIs). For example:

- Reading account details uses `BAPI_USER_GET_DETAIL`.

© 2026 Delorion B.V. All rights reserved.

- Changing account details uses `BAPI_USER_CHANGE`.

SAP identity and permissions

Each connection identifies a SAP system, client and logon user. The authentication method determines how that user signs in:

- **Password authentication:** the administrator supplies their SAP user ID and password for that client.
- **SNC single sign-on:** SAP maps the sign-on identity to a SAP user.

All requests run with that SAP user's normal administration permissions: access to read user and role information and make the user changes assigned to the administrator. The same scope of permitted users, roles and activities applies when working through userXpress.

Connections and global tables

- The **Control Panel** lists the connections.
- The **Global User Table** combines users from the connected clients.
- The **Global Role Table** combines roles from the connected clients.

An account is identified by its system, client and user ID. For example, `DEMO_USER` in client `100` and `DEMO_USER` in client `200` are separate accounts. Changing one does not change the other.

Refresh and operation results

The tables show information retrieved from SAP. They do not continuously reflect changes made by other administrators.

- Refresh the relevant records when you need current values.
- After an operation, check its results for each target. One client can succeed while another fails.
- If a change succeeds but the refresh fails, the displayed information may be old. Check SAP before repeating the change.

SAP GUI and SNC

userXpress reads the SAP Logon configuration selected in **Settings → Connections → SAP Logon configuration**.

SU01 and **PFCG** open selected accounts and roles in SAP GUI while you continue working in userXpress. Set their shared window limit in Settings → Connections → SAP GUI.

Secure Network Communications (SNC) protects communication according to the connection's quality-of-protection setting: authentication, integrity or encryption. SNC can also provide single sign-on when configured for that purpose.

Install your organization's SNC provider, configure its identity and trust, and select its 32-bit library in userXpress. See Configure SNC.

© 2026 Delorion B.V. All rights reserved.

Installation sequence

1. Prepare the workstation using System requirements and compatibility. Install and configure SAP GUI and your SNC provider where required.
2. Install userXpress. Start it under your normal Windows account, set the local passphrase and enter the license.
3. Have your SAP security administrator assign SAP permissions for the work the administrator will perform.
4. Configure the SAP connection. userXpress detects the SAP Logon configuration file automatically. Configure SNC if used, and connect one system/client.

What to configure on each workstation

Program files are installed for the machine. Passphrase, saved logons, queries and preferences belong to the Windows user.

Complete first-start configuration in that person's Windows session, even when IT installs the program centrally.

The local passphrase unlocks userXpress and protects saved SAP logon credentials. SAP passwords or SNC/SSO authenticate the SAP connections. Resetting one does not reset the other. See Storage for storage locations and password-reset consequences.

Online Help opens in the browser. Support requests use the browser and the application to sign in and send the files the administrator approves.

Configure these HTTPS connections separately from SAP access. The network reference lists the destinations.

© 2026 Delorion B.V. All rights reserved.

System requirements and compatibility

Applies to userXpress 2.0.0.0

Prepare the desktop and SAP authorizations required to install and use userXpress.

Desktop requirements

Requirement	What to provide
Operating system	Windows 11 Pro, Enterprise or Education, on a version supported by Microsoft and SAP. Run userXpress under your normal Windows user account.
Memory	At least **2 GB of available RAM for userXpress**, in addition to memory used by Windows, SAP GUI and other applications.
.NET runtime	Microsoft .NET Framework 4.8 or 4.8.1, included with Windows 11.
SAP GUI	A release of SAP GUI for Windows that SAP supports on your Windows version. See SAP GUI and SNC.
Application architecture	userXpress is a 32-bit application. Supply a 32-bit SNC library when using SNC, including on 64-bit Windows.
Installation rights	Windows administrator rights for the machine-wide installation.
SAP connection list	A readable SAP Logon configuration file containing the systems the administrator needs. See SAP Logon connection file.
Network	Workstation access to the SAP servers and SAProuter used by those connections. Online Help and support also need HTTPS access. See Network access.
Personal storage	Write access to the user's settings and cache folders, and to any folder used for workbooks, exports or reports.

SAP GUI and SNC

userXpress follows SAP's maintenance policy for SAP GUI for Windows. Use a release and Windows combination supported in SAP's Lifetime and Support Matrix.

The matrix lists SAP GUI 8.00 and 8.10 for Windows 11. Both the SAP GUI release and the operating system must remain within their supported lifetimes.

Before installing or upgrading SAP GUI, check SAP Note 1053737 for patch availability. You may need an SAP Support Portal account to read it.

- Patches are cumulative. Each patch includes the corrections from earlier patches for that release.
- Use a released patch that SAP has not withdrawn.

© 2026 Delorion B.V. All rights reserved.

- Treat expected shipment dates as estimates, not confirmation that a patch is available.

Install and configure SAP GUI for users who will open **SU01** or **PFCG** from userXpress. Their SAP connections must use Dialog users authorized for those transactions in the target clients.

The SAP RFC runtime must match the userXpress application architecture. If a required library is missing at startup, the error message identifies its filename and architecture.

For SNC, install your organization's SNC provider and configure its identity and trust settings before selecting the library in userXpress.

The library is a Windows DLL. Its architecture must match userXpress, so a 64-bit DLL cannot be used by the 32-bit application. Follow Configure SNC to select the correct file.

Keep the SAP connection components included with userXpress together in the installation directory. Replacing individual DLLs can leave the application with incompatible components.

Storage and rollout preparation

Memory use increases with the number of users and roles loaded and the operations performed. Check memory availability with the intended SAP clients connected before rolling out to all administrators.

Allow disk space for local settings and caches, exported workbooks and diagnostic reports.

Exports and account-creation workbooks can contain personal information and passwords. Choose their storage locations before introducing the application into daily use.

Continue with Installation and enterprise deployment.

SAP requirements

userXpress uses the SAP authorizations an administrator normally needs for user administration:

- Read user and role information, including account details and assignments.
- Update users according to the administrator's responsibilities, such as changing account details, resetting passwords or assigning roles.

Using userXpress does not require broader administrative privileges. The administrator's existing scope of permitted users, roles and activities continues to apply.

Use a personal SAP account in each system/client the administrator manages. For SNC single sign-on, these permissions belong to the SAP user mapped to that identity.

The reference below gives the SAP security administrator a complete picture of the RFC calls, table reads and administration permissions used by these tasks. Use it to map the administrator's existing responsibilities to SAP authorization fields. Entries for specialized tasks, such as maintaining role definitions, apply to administrators who perform those tasks.

In the examples, `*` means all values for a field. Use the user groups, role names and other values from your organization's authorization model.

© 2026 Delorion B.V. All rights reserved.

RFC and table access

In **S_RFC**, maintain `ACTVT = 16` for execution. Use `RFC_TYPE = FUNC` to name individual remote function modules, or `RFC_TYPE = FUGR` for function groups. `RFC_NAME` contains the corresponding function or group names.

A function-group grant covers the group's functions and can therefore be broader than an individual-function grant. See SAP's S_RFC reference.

Authorization object and field	Values and purpose
`S_RFC.ACTVT`	`16` — execute remote function calls.
`S_RFC.RFC_TYPE`	`FUNC` — individual functions.
`S_RFC.RFC_NAME`	Functions for the permitted operations, listed in RFC execution and administration permissions. Include supporting metadata and table-read calls described below.
`S_RFC.RFC_TYPE` / `RFC_NAME`	Where function-group grants are used: `FUGR` with `RFC1`, `STFC`, `SYST`. Keep these in a separate authorization instance from the `FUNC` entries.
`S_TABU_NAM.ACTVT`	`03` — display table contents.
`S_TABU_NAM.TABLE`	The table names needed for the selected features, grouped below. This permission does not grant table maintenance.

Common supporting RFCs include `RFC_READ_TABLE`, `DDIF_FIELDINFO_GET`, `RFC_GET_FUNCTION_INTERFACE`, `RFC_SYSTEM_INFO` and `RFCPING`. The required calls depend on the operation and the SAP system.

For a rejected supporting call, an authorization trace identifies the permission involved.

Maintain table-read access by purpose:

- **Users, addresses and assignments:** `ADCP`, `ADR6`, `ADRC`, `AGR_USERS`, `DEVACCESS`, `USCOMPANY`, `USER_ADDRP`, `USGRP`, `USGRPT`, `USR01`, `USR02`, `USR05`, `USR06`, `USR10`, `USR21`, `USR41`, `USRACL`, `USREFUS`.
- **Roles and their content:** `AGR_AGRS`, `AGR_DEFINE`, `AGR_TEXTS`, `AGR_MINI`, `AGR_MINIT`, `AGR_TCODES`, `AGR_TIME`, `AGR_CUSTOM`, `AGR_1250`, `AGR_1251`, `AGR_ATTS`, `AGR_BUFFI`, `AGR_1253`, `AGR_1252`, `AGR_HIERT`, `AGR_HIER`, `AGR_FLAGS`, `AGR_LSD`, `AGR_HPAGE`, `AGR_MAPP`.
- **System and user reference values:** `CVERS_TXT`, `DD02L`, `SA`, `SEC_POLICY_CUST`, `SVERS`, `T000`, `T005K`, `T005T`, `TBDLST`, `TPARA`, `TPARAT`, `TSACT`, `TSAD2`, `TSAD3`, `TSAD3T`, `TSP03`, `TUTYP`, `TUTYPA`, `TUTYPNOW`, `USRFLDDEF`, `USRFLDGRP`, `USRFLDSEL`, `USRFLDT`, `USZBVSYS`.
- **Role content filter metadata:** `TSTC`, `TSTCT`, `TOBJ`, `TOBJT`, `AUTHX`, `DD04T`, `TACT`, `TACTT`, `TACTZ`, `DD04L`, `DD01L`, `DD07L`, `DD07T`, `DD08L`, `DD05M`. Value suggestions can also read the check or text table associated with the selected authorization field.

© 2026 Delorion B.V. All rights reserved.

SAP applies table authorization groups and other configured checks according to its release and configuration. Match table-read access to the user and role information needed for the administrator's tasks.

User administration

The values below describe standard SAP administration capabilities. Choose the activities that match the administrator's duties. Display-only users need the corresponding read access.

`ACTVT` identifies the permitted activity. Each code is shown with its meaning below. The scope fields define which users, roles, profiles or values those activities may affect.

Object	Scope fields	ACTVT — activity
S_USER_GRP	`CLASS` = `*`. Controls user administration within the permitted user groups.	`01` — Create `02` — Change `03` — Display `05` — Lock or unlock users and change passwords `06` — Delete `08` — Display change documents `22` — Enter, include or assign `24` — Archive
S_USER_AGR	`ACT_GROUP` = `*`. Controls role administration and assignment activities for the permitted roles.	`02` — Change `03` — Display `21` — Transport `22` — Enter, include or assign `36` — Extended maintenance `64` — Generate authorization profiles
S_USER_PRO	`PROFILE` = `*`. Controls administration and assignment of authorization profiles.	`01` — Create `02` — Change `03` — Display `06` — Delete `07` — Activate `08` — Display change documents `22` — Enter, include or assign
S_USER_AUT	`OBJECT` = `*` `AUTH` = `*`. Controls work with authorizations for the permitted authorization objects and authorization names.	`01` — Create `02` — Change `03` — Display `06` — Delete `07` — Activate `08` — Display change documents `22` — Enter, include or assign

S_USER_SAS	`ACT_GROUP` = `*`
	`CLASS` = `*`
	`PROFILE` = `*`
	`SUBSYSTEM` = `*`. Controls assignment scope where the corresponding SAP assignment checks are active.
		`22` — Enter, include or assign

© 2026 Delorion B.V. All rights reserved.

Object	Scope fields	ACTVT — activity
S_USER_SYS	SUBSYSTEM = *. Applies to system assignments in Central User Administration (CUA).	78 — Assign
S_USER_TCD	TCD = *. Defines transaction codes the administrator may include in roles. It does not grant permission to start those transactions.	—
S_USER_VAL	OBJECT = * AUTH_FIELD = * AUTH_VALUE = *. Defines authorization field values the administrator may maintain.	—
S_SECPOL	POLICYNAME = *. Permits assignment of the specified security policies.	22 — Enter, include or assign
S_ADDRESS1	ADGRP = BC01. Permits the corresponding user-address operations.	01 — Create 02 — Change 03 — Display 06 — Delete

Use the administrator's established scope in place of the wildcard examples:

- Replace `S_USER_AGR.ACT_GROUP = *` with approved role names or a pattern such as `Z_FIN_*`.
- Replace `S_USER_GRP.CLASS = *` with the user groups the administrator manages, such as `FINANCE`.

Apply the same role names, user groups and activities in related assignment objects such as `S_USER_SAS`.

Read access and change access have their own SAP authorization checks. Configure each for the information the administrator may view and the users they may maintain.

Opening `SU01` or `PFCG` from userXpress uses the same **S_TCODE** and display or maintenance permissions as opening those transactions directly in SAP GUI.

Use existing SAP roles that provide this access, or the supplied userXpress role package. The role guide explains profile generation, assignment and user comparison when using the package.

© 2026 Delorion B.V. All rights reserved.

Audit

Applies to userXpress 2.0.0.0

Find SAP user and role change documents and identify the SAP account that performed a change.

Which user performs an action?

Every request userXpress sends to SAP runs under the SAP user authenticated for that connection. With SNC single sign-on, this is the SAP user mapped to the sign-on identity. SAP records that account as the actor for changes that generate change documents.

Use each administrator's own SAP account so that changes can be attributed to that person. If several people use the same SAP account, the SAP user name alone cannot distinguish them.

The Windows account and local userXpress passphrase do not replace the SAP identity in these records.

Find changes to users

1. Open **SU01** in the SAP system and client where the change was made.
2. Choose **Information → Change Documents for Users**.
3. Enter the affected user and the relevant date/time range. To investigate one administrator's work, also restrict the selection to that administrator's SAP user where the selection screen offers it.
4. Execute the selection and open the relevant change documents. Compare the recorded actor, time and changed fields with the operation you are investigating.

User change documents can include account attributes, validity, user-group and assignment changes. Password-related changes can be recorded, but the password itself is not a readable audit value.

Available selections and document detail depend on the SAP release. See SAP's SU01 documentation.

Find changes to roles

1. Open **PFCG** in the SAP system and client where the role is maintained.
2. Enter the role name, then choose **Environment → Display Changes**.
3. Restrict the selection by role, date and changed-by user as needed. Select the change-document categories relevant to the investigation and execute the selection.
4. Open the matching documents to inspect the recorded changes. Role content changes and user-assignment changes answer different questions. Include both categories when investigating a change in a user's access.

© 2026 Delorion B.V. All rights reserved.

The menu is described in SAP's role administration reference.

SAP also provides the role change-document report through **SUIM → Change Documents → For Roles**. See Displaying Change Documents for Roles.

What these records establish

For logons, failed authorization checks or other security events, use your organization's SAP security logging and tracing procedures.

If an expected change is absent, first confirm the SAP system, client, affected user or role, date range and connection account. Check the userXpress operation result to establish whether SAP accepted the change.

For an authorization failure, follow Diagnose a SAP authorization failure. Local application logs can help correlate an error, but do not replace SAP's change documents or your SAP audit-retention policy.

© 2026 Delorion B.V. All rights reserved.

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

© 2026 Delorion B.V. All rights reserved.

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.

© 2026 Delorion B.V. All rights reserved.

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.

© 2026 Delorion B.V. All rights reserved.

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.

© 2026 Delorion B.V. All rights reserved.