Technical Documentation

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- Use a released patch that SAP has not withdrawn.
- 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.

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.

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

Object	Scope fields	ACTVT — activity

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

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.