Required SAP access

Applies to userXpress 2.0.0.0

Understand the SAP permissions used by userXpress and trace an authorization failure to the affected account and operation.

Which account needs access?

userXpress works with the permissions of the SAP user used for each connection. For SNC single sign-on, this is the SAP account mapped to that identity.

The administrator needs the normal SAP access for their work: reading user and role information and updating users within their assigned responsibilities. Using userXpress keeps that administrative scope unchanged.

This page explains how those permissions apply to the SAP calls behind each task. It provides a reference for the SAP security administrator and a procedure for resolving an authorization error. For authorization objects, fields and values, see SAP requirements.

RFC execution and administration permissions

SAP uses **S_RFC** to control execution of remote function calls. The role must allow the required functions or function groups for your SAP release.

SAP checks RFC execution permission together with the user, role or table permissions for the requested task. See SAP RFC authorization.

The following reference maps administration tasks to their principal SAP calls. Use the entries relevant to the administrator's work.

Each task includes the supporting reads needed to display account details, offer field values and refresh the result after a change.

Task	Principal SAP calls
Read account details	`BAPI_USER_GET_DETAIL`, together with user, address and assignment table reads.
Create, change or delete accounts	`BAPI_USER_CREATE1`, `BAPI_USER_CHANGE`, `BAPI_USER_DELETE`.
Lock or unlock accounts	`BAPI_USER_LOCK`, `BAPI_USER_UNLOCK`.
Set initial or deactivate passwords	`BAPI_USER_CHANGE`.
Set productive passwords	`SUSR_USER_CHANGE_PASSWORD_RFC`. Password generation/checking also uses `SUSR_GENERATE_PASSWORD` and `PASSWORD_FORMAL_CHECK`.

Task	Principal SAP calls
Assign roles or profiles	`BAPI_USER_ACTGROUPS_ASSIGN`, `BAPI_USER_PROFILES_ASSIGN`, plus reads of existing assignments.
Copy role definitions and generate profiles	`/SDF/PRGN_EXECUTE_UPLOAD`, `PRGN_AUTO_GENERATE_PROFILE_NEW`.
Send a message or end a SAP session	`TH_POPUP` for messages. `TH_DELETE_USER` for session termination.

User administration involves **S_USER_GRP** for user-group scope. Role administration involves **S_USER_AGR**. Profile and assignment operations can additionally involve **S_USER_PRO** and **S_USER_SAS**, depending on your SAP authorization-check configuration.

Use the groups, roles, profiles and activities already defined for the administrator's responsibilities. SAP describes these checks in its user administration and role administration guidance.

SAP controls read access and change access through their respective authorization checks. Set the scope of each according to the administrator's responsibilities.

Access for role content filters

Role content searches read the authorization data maintained in roles, including authorization headers (`AGR_1250`), field values (`AGR_1251`), organizational values (`AGR_1252`) and role-menu data.

The editor also reads authorization and dictionary metadata to describe fields and suggest values. Some value lists require access to a field's own check table.

When access to one of these sources fails, the search can show confirmed matches alongside roles it could not evaluate. Those unverified roles are not confirmed non-matches.

Open **Details…** for the failed reads, correct the permission or connection problem and use **Run again**.

A match describes maintained role content. It does not establish that a particular user can execute a transaction: assignments, validity, generated profiles and other SAP checks also affect that user's access.

SAP GUI transactions

Commands such as **SU01** open SAP GUI using the account's normal transaction access and display or maintenance permissions, just as when the administrator opens the transaction directly.

Diagnose a SAP authorization failure

1. Record the exact error, action, time, SAP logon user, system and client. Include the function or table named in the error.
2. Have the SAP security administrator activate an authorization trace for that user, covering the application server handling the RFC request. **STAUTHTRACE** or **ST01** can be used according to the SAP release and your tracing procedure.

3. Reproduce the failing action once, then stop the trace. For an action that changes SAP data, first check whether the original attempt already made the change.
4. Inspect the failed authorization checks and their field values. Correct the intended role, regenerate the profile and complete user comparison where required.
5. Reconnect userXpress and repeat the affected action.

SAP's authorization trace guidance explains trace scope. A trace on a different application server can miss the RFC request.

If the action succeeded but updating the table failed, investigate the refresh read separately. Repeating a successful account change will not fix a missing read authorization.