

Restricting Registration of DataBlade Modules and UDRs

What is restricting registration of DataBlade modules and UDRs?

You can restrict registration of DataBlade modules and UDRs to improve security and to control accessibility. User-defined routines (UDR) can use shared-object (library) files that are external to the database server which could potentially contain harmful code. The Database Server Administrator (DBSA) can use a new built-in role, called EXTEND, to specify which users can register, drop, or replace DataBlade and UDRs that include the EXTERNAL NAME clause.

What restricted registration does

The DBSA can use the GRANT statement to confer the EXTEND role on a user, or can use REVOKE to withdraw that role from a user to prevent unauthorized user from registering DataBlade UDRs.

How to use restricted registration and ROLES

A new configuration parameter, IFX_EXTEND_ROLE, has been introduced to enable a DBSA to prevent unauthorized users from registering DataBlade UDRs. The default value of the IFX_EXTEND_ROLE configuration parameter is OFF.

After setting the IFX_EXTEND_ROLE configuration parameter to ON, the DBSA uses the following syntax to grant and revoke privileges to and from specific users:

```
GRANT EXTEND TO username
REVOKE EXTEND FROM username
username
```

The name of the user to grant or revoke privileges

The grant/revoke EXTEND role to a specific user will update the sysroleauth system catalog table.

The DBSA can disable this feature by setting IFX_EXTEND_ROLE configuration parameter to OFF. If the IFX_EXTEND_ROLE configuration parameter is set to OFF, the EXTEND role is not operational and any user can register external routines.

If you have privileges to register a UDR or if the IFX_EXTEND_ROLE configuration parameter is set to OFF and you are responsible for registering UDRs, you must register UDRs in all databases in which they will be used, unless the database is on the secondary database server of an HDR pair.