Snowflake ROLE

Snowflake Documentation

- Overview of Access Control
- CREATE ROLE
- GRANT <Privileges> TO ROLE
- Configuring Access Control

Active Roles

Database	Role Type	Role Name	Role Description
ALL	System-Defined	ORGADMIN	(aka Organization Administrator) Role that manages operations at the organization level. More specifically, this role: • Can create accounts in the organization. • Can view all accounts in the organization (using SHOW ORGANIZATION ACCOUNTS) as well as all regions enabled for the organization (using SHOW REGIONS). • Can view usage information across the organization.
ALL	System-Defined	ACCOUNTADMIN	(aka Account Administrator)

			Role that encapsulates the SYSADMIN and SECURITYADMIN system-defined roles. It is the top-level role in the system and should be granted only to a limited/controlled number of users in your account
ALL	System-Defined	SECURITYADMIN	(aka Security Administrator) Role that can manage any object grant globally, as well as create, monitor, and manage users and roles. More specifically, this role: - Is granted the MANAGE GRANTS security privilege to be able to modify any grant, including revoking it. - Inherits the privileges of the USERADMIN role via the system role hierarchy (i.e. USERADMIN role is granted to SECURITYADMIN).
ALL	System-Defined	USERADMIN	(aka User and Role Administrator) Role that is dedicated to user and role management only. More specifically, this role: - Is granted the CREATE USER and CREATE ROLE security privileges. - Can create users and roles in the account. - This role can also manage users and roles that it owns. Only the role with the OWNERSHIP privilege on an object (i.e. user or role), or a higher role, can modify the object properties.
ALL	System-Defined	SYSADMIN	(aka System Administrator) Role that has privileges to create warehouses, databases, schemas, tables, views, tasks, and other objects in an account. If, as recommended, you create a role hierarchy that ultimately assigns all custom roles to the SYSADMIN role, this role also has the ability to grant privileges on warehouses,

			databases, and other objects to other roles.
DB_KKF_CHAINACCOUNT	Custom	RL_PROJECTADMIN	(aka Project Administrator - Chain Accounts) Role that has privileges to create schemas, tables and views in the DB_KKC_CHAINACCOUNT database.
DB_KKF_MAIN	Custom	RL_POWERBIADMIN	(aka Power BI Administrator) Role that has privileges to read tables and views in the DB_KKF_MAIN and DB_KKF_CHAINACCOUNT databases. This role acts as a service account utilized by Power BI, since Power BI only needs read privileges to specific data objects within the DB_KKF_MAIN and DB_KKF_CHAINACCOUNT databases.
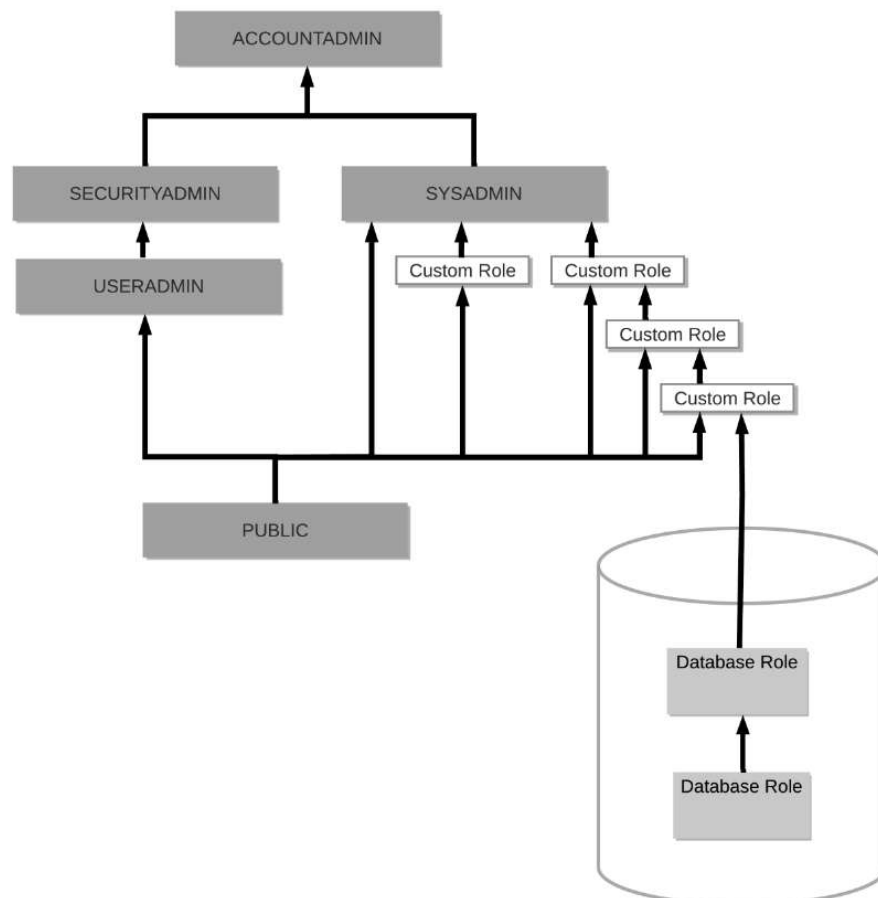
⌃   CREATE ROLE Template

```
1 -- Only the USERADMIN role, or a higher role, has this privilege by default. The privilege
  can be granted to additional roles as needed
2 USE ROLE USERADMIN;
3
4 -- Proper naming convention for creating a role is to prepend "RL_" before the role name
  (i.e. RL_PROJECT_ADMIN)
5 CREATE OR REPLACE ROLE RL_<Role_Name>;
```

⌃   Grant a role access to the specified Snowflake Warehouse

```
1 USE ROLE SECURITYADMIN;
2
3 GRANT USAGE ON WAREHOUSE <Warehouse_Name>
4 TO ROLE <Role_Name>;
```

⌃   Grant a role access to the specified Snowflake Database

```
1 USE ROLE SECURITYADMIN;
2
3 GRANT USAGE ON DATABASE <Database_Name>
4 TO ROLE <Role_Name>;
```

⌃   Grant a role access to the specified Snowflake Schema

```
1 USE ROLE SECURITYADMIN;
2
3 GRANT USAGE ON SCHEMA <Database_Name>.<Schema_Name>
```

```
4 TO ROLE <Role_Name>;
```

∧ Grant a role privileges to the specified Snowflake Table/View

```
1 USE ROLE SECURITYADMIN;
2
3 GRANT <privilege> ON TABLE/VIEW <Database_Name>.<Schema_Name>.<Table/View_Name>
4 TO ROLE <Role_Name>;
```

∧ Grant a user access to a specific Snowflake role

```
1 USE ROLE SECURITYADMIN;
2
3 GRANT ROLE <Role_Name>
4 TO USER <User_Name>;
```

∧ Grant additional privileges to a specific Snowflake role

```
 1 USE ROLE SECURITYADMIN;
 2
 3 --
 4 GRANT <Account_Object_Privileges>
 5     ON <Account_Object> <Account_Object_Name>
 6     TO ROLE <Role_Name>
 7         /*
 8             Account Object & Privileges:
 9             -
10         */
11 ;
12
13
14
15 --
16 GRANT <Schema_Privileges>
17     ON SCHEMA <Database_Name>.<Schema_Name>
18     TO ROLE <Role_Name>
19         /*
```

```
20              Schema Privileges:
21                  -
22          */
23  ;
24
25
26
27  --
28  GRANT <Schema_Privileges>
29      ON ALL SCHEMAS IN DATABASE <Database_Name>
30      TO ROLE <Role_Name>
31          /*
32              Schema Privileges:
33                  -
34          */
35  ;
36
37
38
39  --
40  GRANT <Schema_Privileges>
41      ON FUTURE SCHEMAS IN DATABASE <Database_Name>
42      TO ROLE <Role_Name>
43          /*
44              Schema Privileges:
45                  -
46          */
47  ;
48
49
50
51  --
52  GRANT <Schema_Object_Privileges>
53      ON <Object_Type> <Object_Name>
54      TO ROLE <Role_Name>
55          /*
56              Schema Object & Privileges:
57                  -
58          */
59  ;
60
61
62
63  --
64  GRANT <Schema_Object_Privileges>
65      ON ALL <Object_Type_Plural>
66      IN DATABASE <Database_Name>
67      TO ROLE <Role_Name>
68          /*
69              Object Type & Privileges:
70                  -
71          */
72  ;
73
74
75
76  --
77  GRANT <Schema_Object_Privileges>
78      ON ALL <Object_Type_Plural>
79      IN SCHEMA <Database_Name>.<Schema_Name>
80      TO ROLE <Role_Name>
81          /*
82              Object Type & Privileges:
```

```
 83                  -
 84          */
 85 ;
 86
 87
 88
 89 --
 90 GRANT <Schema_Object_Privileges>
 91     ON FUTURE <Object_Type_Plural>
 92     IN DATABASE <Database_Name>
 93     TO ROLE <Role_Name>
 94         /*
 95             Object Type & Privileges:
 96                 -
 97         */
 98 ;
 99
100
101
102 --
103 GRANT <Schema_Object_Privileges>
104     ON FUTURE <Object_Type_Plural>
105     IN SCHEMA <Database_Name>.<Schema_Name>
106     TO ROLE <Role_Name>
107         /*
108             Object Type & Privileges:
109                 -
110         */
111 ;
```

Edit   **Contact Intranet Support**