# Snowflake Streamlit App Roles and Privileges

## Overview

This document explains the role-based access control for Snowflake Streamlit applications, focusing on the distinction between OWNER and READ roles, and the specific privileges required for different Streamlit operations.

## Role Distinctions

### OWNER Role

The **OWNER** role provides full administrative control over a Streamlit application.

| **Capability** | **Description** |
| --- | --- |
| **Full Control** | Complete administrative access to the Streamlit app |
| **Modify Code** | Can edit, update, and deploy new versions of the app |
| **Manage Access** | Can grant and revoke permissions to other users/roles |
| **Delete App** | Can permanently delete the Streamlit application |
| **View Logs** | Access to application logs and debugging information |
| **Configuration** | Can modify app settings, environment variables, and configurations |
| **Deployment** | Can deploy, redeploy, and manage app versions |

### READ Role

The **READ** role provides view-only access to a Streamlit application.

| **Capability** | **Description** |
| --- | --- |
| **View Only** | Can access and interact with the Streamlit app interface |
| **Execute Functions** | Can use app functionality (buttons, inputs, queries) |
| **No Modifications** | Cannot edit code, settings, or configurations |
| **No Admin Access** | Cannot manage permissions or delete the app |
| **Limited Visibility** | No access to source code or administrative features |

## Key Differences Summary

| **Aspect** | **OWNER Role** | **READ Role** |
| --- | --- | --- |
| **App Access** | ✅ Full Access | ✅ View/Use Only |
| **Code Editing** | ✅ Yes | ❌ No |
| **Permission Management** | ✅ Yes | ❌ No |
| **App Deletion** | ✅ Yes | ❌ No |
| **Configuration Changes** | ✅ Yes | ❌ No |
| **Log Access** | ✅ Yes | ❌ No |
| **Deployment Control** | ✅ Yes | ❌ No |

## Required Privileges for Streamlit Operations

### 1. Creating a Streamlit App

To create a new Streamlit application, a user/role must have the following privileges:

#### Database and Schema Privileges

-- Database level privileges  
GRANT USAGE ON DATABASE <database\_name> TO ROLE <role\_name>;  
GRANT CREATE STREAMLIT ON DATABASE <database\_name> TO ROLE <role\_name>;  
  
-- Schema level privileges   
GRANT USAGE ON SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;  
GRANT CREATE STREAMLIT ON SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;

#### Warehouse Privileges

-- Warehouse access for app execution  
GRANT USAGE ON WAREHOUSE <warehouse\_name> TO ROLE <role\_name>;  
GRANT OPERATE ON WAREHOUSE <warehouse\_name> TO ROLE <role\_name>;

#### Additional Requirements

* **Role Assignment:** User must be assigned a role with the above privileges
* **Stage Access:** If using external files, appropriate stage privileges are required
* **Compute Resources:** Access to a warehouse for app execution

#### Example: Complete Setup for App Creation

-- Create a role for Streamlit developers  
CREATE ROLE STREAMLIT\_DEVELOPER;  
  
-- Grant database and schema privileges  
GRANT USAGE ON DATABASE ANALYTICS TO ROLE STREAMLIT\_DEVELOPER;  
GRANT CREATE STREAMLIT ON DATABASE ANALYTICS TO ROLE STREAMLIT\_DEVELOPER;  
GRANT USAGE ON SCHEMA ANALYTICS.APPS TO ROLE STREAMLIT\_DEVELOPER;  
GRANT CREATE STREAMLIT ON SCHEMA ANALYTICS.APPS TO ROLE STREAMLIT\_DEVELOPER;  
  
-- Grant warehouse privileges  
GRANT USAGE ON WAREHOUSE COMPUTE\_WH TO ROLE STREAMLIT\_DEVELOPER;  
GRANT OPERATE ON WAREHOUSE COMPUTE\_WH TO ROLE STREAMLIT\_DEVELOPER;  
  
-- Assign role to user  
GRANT ROLE STREAMLIT\_DEVELOPER TO USER john\_doe;

### 2. Editing a Streamlit App

To edit an existing Streamlit application, a user/role needs:

#### Ownership or Explicit Privileges

-- Option A: Transfer ownership  
GRANT OWNERSHIP ON STREAMLIT <database\_name>.<schema\_name>.<app\_name>   
TO ROLE <role\_name> REVOKE CURRENT GRANTS;  
  
-- Option B: Grant modify privileges (if supported)  
GRANT MODIFY ON STREAMLIT <database\_name>.<schema\_name>.<app\_name>   
TO ROLE <role\_name>;

#### Underlying Resource Access

-- Database and schema access  
GRANT USAGE ON DATABASE <database\_name> TO ROLE <role\_name>;  
GRANT USAGE ON SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;  
  
-- Warehouse access for testing changes  
GRANT USAGE ON WAREHOUSE <warehouse\_name> TO ROLE <role\_name>;  
GRANT OPERATE ON WAREHOUSE <warehouse\_name> TO ROLE <role\_name>;

#### Data Access (if app queries data)

-- Table/view privileges for data access  
GRANT SELECT ON TABLE <database\_name>.<schema\_name>.<table\_name> TO ROLE <role\_name>;  
GRANT SELECT ON ALL TABLES IN SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;  
  
-- Future grants for new tables  
GRANT SELECT ON FUTURE TABLES IN SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;

#### Example: Setup for App Editing

-- Create role for app editors  
CREATE ROLE STREAMLIT\_EDITOR;  
  
-- Grant ownership of specific app  
GRANT OWNERSHIP ON STREAMLIT ANALYTICS.APPS.SALES\_DASHBOARD   
TO ROLE STREAMLIT\_EDITOR REVOKE CURRENT GRANTS;  
  
-- Grant necessary resource access  
GRANT USAGE ON DATABASE ANALYTICS TO ROLE STREAMLIT\_EDITOR;  
GRANT USAGE ON SCHEMA ANALYTICS.APPS TO ROLE STREAMLIT\_EDITOR;  
GRANT USAGE ON WAREHOUSE COMPUTE\_WH TO ROLE STREAMLIT\_EDITOR;  
  
-- Grant data access  
GRANT SELECT ON ALL TABLES IN SCHEMA ANALYTICS.SALES TO ROLE STREAMLIT\_EDITOR;  
  
-- Assign to user  
GRANT ROLE STREAMLIT\_EDITOR TO USER jane\_smith;

### 3. Viewing a Streamlit App

To view and use a Streamlit application, a user/role needs minimal privileges:

#### App Access Privileges

-- Basic app access  
GRANT USAGE ON STREAMLIT <database\_name>.<schema\_name>.<app\_name>   
TO ROLE <role\_name>;

#### Database and Schema Access

-- Database access  
GRANT USAGE ON DATABASE <database\_name> TO ROLE <role\_name>;  
  
-- Schema access  
GRANT USAGE ON SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;

#### Warehouse Access (for app execution)

-- Warehouse usage for running the app  
GRANT USAGE ON WAREHOUSE <warehouse\_name> TO ROLE <role\_name>;

#### Data Access (if app displays data)

-- Read access to underlying data  
GRANT SELECT ON TABLE <database\_name>.<schema\_name>.<table\_name> TO ROLE <role\_name>;  
  
-- Or schema-level access  
GRANT SELECT ON ALL TABLES IN SCHEMA <database\_name>.<schema\_name> TO ROLE <role\_name>;

#### Example: Setup for App Viewing

-- Create role for app viewers  
CREATE ROLE STREAMLIT\_VIEWER;  
  
-- Grant app access  
GRANT USAGE ON STREAMLIT ANALYTICS.APPS.SALES\_DASHBOARD TO ROLE STREAMLIT\_VIEWER;  
  
-- Grant resource access  
GRANT USAGE ON DATABASE ANALYTICS TO ROLE STREAMLIT\_VIEWER;  
GRANT USAGE ON SCHEMA ANALYTICS.APPS TO ROLE STREAMLIT\_VIEWER;  
GRANT USAGE ON WAREHOUSE COMPUTE\_WH TO ROLE STREAMLIT\_VIEWER;  
  
-- Grant data access (read-only)  
GRANT SELECT ON ALL TABLES IN SCHEMA ANALYTICS.SALES TO ROLE STREAMLIT\_VIEWER;  
  
-- Assign to users  
GRANT ROLE STREAMLIT\_VIEWER TO USER viewer1;  
GRANT ROLE STREAMLIT\_VIEWER TO USER viewer2;

## Privilege Hierarchy and Best Practices

### Recommended Role Structure

-- 1. Streamlit Admin Role (Full Control)  
CREATE ROLE STREAMLIT\_ADMIN;  
GRANT CREATE STREAMLIT ON DATABASE ANALYTICS TO ROLE STREAMLIT\_ADMIN;  
GRANT USAGE ON ALL WAREHOUSES TO ROLE STREAMLIT\_ADMIN;  
  
-- 2. Streamlit Developer Role (Create & Edit)  
CREATE ROLE STREAMLIT\_DEVELOPER;  
GRANT CREATE STREAMLIT ON SCHEMA ANALYTICS.APPS TO ROLE STREAMLIT\_DEVELOPER;  
GRANT USAGE ON WAREHOUSE DEV\_WH TO ROLE STREAMLIT\_DEVELOPER;  
  
-- 3. Streamlit Editor Role (Edit Specific Apps)  
CREATE ROLE STREAMLIT\_EDITOR;  
-- Grant ownership on specific apps as needed  
  
-- 4. Streamlit Viewer Role (Read-Only Access)  
CREATE ROLE STREAMLIT\_VIEWER;  
GRANT USAGE ON WAREHOUSE VIEWER\_WH TO ROLE STREAMLIT\_VIEWER;

### Security Best Practices

#### Principle of Least Privilege

* Grant only the minimum privileges required for each role
* Use specific object grants rather than broad schema-level grants when possible
* Regularly audit and review granted privileges

#### Role Separation

* **Separate development and production environments**
* **Use different roles for different environments**
* **Limit production access to authorized personnel only**

## Common Scenarios and Solutions

### Scenario 1: User Cannot Create Streamlit App

**Problem:** User gets “Insufficient privileges” error when creating app

**Solution:**

-- Check current privileges  
SHOW GRANTS TO USER <username>;  
  
-- Grant required privileges  
GRANT USAGE ON DATABASE <db\_name> TO ROLE <user\_role>;  
GRANT CREATE STREAMLIT ON SCHEMA <db\_name>.<schema\_name> TO ROLE <user\_role>;  
GRANT USAGE ON WAREHOUSE <wh\_name> TO ROLE <user\_role>;

### Scenario 2: User Can View But Cannot Edit App

**Problem:** User can access app but cannot modify code

**Solution:**

-- Transfer ownership or grant modify privileges  
GRANT OWNERSHIP ON STREAMLIT <db\_name>.<schema\_name>.<app\_name>   
TO ROLE <user\_role> REVOKE CURRENT GRANTS;

### Scenario 3: App Runs But Cannot Access Data

**Problem:** Streamlit app loads but shows “no data” or permission errors

**Solution:**

-- Grant data access privileges  
GRANT SELECT ON ALL TABLES IN SCHEMA <data\_schema> TO ROLE <app\_role>;  
GRANT SELECT ON ALL VIEWS IN SCHEMA <data\_schema> TO ROLE <app\_role>;  
  
-- For future objects  
GRANT SELECT ON FUTURE TABLES IN SCHEMA <data\_schema> TO ROLE <app\_role>;

### Scenario 4: Performance Issues with Streamlit Apps

**Problem:** Apps run slowly or time out

**Solution:**

-- Ensure adequate warehouse resources  
ALTER WAREHOUSE <warehouse\_name> SET WAREHOUSE\_SIZE = 'MEDIUM';  
  
-- Grant OPERATE privilege for auto-resume  
GRANT OPERATE ON WAREHOUSE <warehouse\_name> TO ROLE <app\_role>;  
  
-- Consider dedicated warehouse for Streamlit apps  
CREATE WAREHOUSE STREAMLIT\_WH WITH   
 WAREHOUSE\_SIZE = 'LARGE'  
 AUTO\_SUSPEND = 300  
 AUTO\_RESUME = TRUE;

## Troubleshooting Guide

### Common Error Messages

| **Error Message** | **Cause** | **Solution** |
| --- | --- | --- |
| “Insufficient privileges to operate on STREAMLIT” | Missing CREATE STREAMLIT privilege | Grant CREATE STREAMLIT on database/schema |
| “Object does not exist or not authorized” | Missing USAGE privilege on app | Grant USAGE on specific Streamlit app |
| “Warehouse not found or not authorized” | Missing warehouse privileges | Grant USAGE and OPERATE on warehouse |
| “SQL compilation error: Object not found” | Missing data access privileges | Grant SELECT on required tables/views |

### Diagnostic Queries

-- Check user's current role and privileges  
SELECT CURRENT\_ROLE(), CURRENT\_USER();  
SHOW GRANTS TO ROLE <role\_name>;  
  
-- Check Streamlit app permissions  
SHOW GRANTS ON STREAMLIT <database>.<schema>.<app\_name>;  
  
-- Check warehouse access  
SHOW GRANTS ON WAREHOUSE <warehouse\_name>;  
  
-- Verify database and schema access  
SHOW GRANTS ON DATABASE <database\_name>;  
SHOW GRANTS ON SCHEMA <database\_name>.<schema\_name>;

## Additional Resources

### Snowflake Documentation

* [Streamlit in Snowflake Documentation](https://docs.snowflake.com/en/developer-guide/streamlit/about-streamlit)
* [Access Control Privileges](https://docs.snowflake.com/en/user-guide/security-access-control-privileges)
* [Role-Based Access Control](https://docs.snowflake.com/en/user-guide/security-access-control-overview)

### Best Practice Guidelines

* Always test privilege grants in a development environment first
* Document role assignments and privilege grants for audit purposes
* Regularly review and clean up unused roles and privileges
* Use resource monitors to control warehouse usage for Streamlit apps