User Role Management

Introduction

An essential component of access control in any system is user role management. A Role-Based Access Control (RBAC) model organizes permissions into predefined roles rather than giving them to individual users. Roles are then allocated to users according to their duties. This method makes administration easier, guarantees scalability, and adheres to the least privilege principle, which states that users should only be granted the minimal amount of access necessary to complete their tasks.

Defined User Roles and Permissions

To manage access well, we set up three basic roles: Viewer, Editor, and Admin. These roles build on each other, so each higher role gets the permissions of the lower ones and gets new ones. This layered structure makes it easier to run the system without compromising security.

1. Viewer

   The most fundamental role is Viewer, which is intended for end users who only require access to consume information and shouldn't tamper with data or system functions. Usually, viewers are stakeholders who need access to reports or dashboards, like managers, auditors, or clients.

   - They can use legitimate login credentials to access the system.
   - They are unable to change reports, dashboards, or content, but they can view and access them.
   - Their read-only access to data guarantees the preservation of system integrity.
   - They are unable to add, edit, remove, or upload records.
   - They are unable to access areas for system configuration or user management.

2. Editor

   The mid-level Editor position is intended for analysts, content producers, and department employees who must engage with the system in ways other than viewing. In order to reduce risks, editors are purposefully prohibited from

managing users or system settings, even though they can contribute value to the system by adding or updating data.

- All Viewer permissions are passed down to editors.
- Reports, documents, and dashboard widgets are examples of the new content they can produce.
- Within their purview, they can alter already-existing records by changing settings, editing entries, or updating a case file.
- They are unable to remove sensitive or permanent datasets, but they can remove some non-essential data, like draft reports or temporary records.
- Editors are unable to assign roles, create or manage user accounts, or change system-wide settings.

3. Admin

   System administrators, IT workers, or other trusted individuals in charge of general governance are usually assigned to the admin role, which offers the highest level of authority in the system. Admins are in charge of user management, security, and compliance and have complete access.

   - All Viewer and Editor permissions are passed down to administrators.
   - They have unrestricted access to create, edit, and remove any kind of data.
   - They are in charge of managing user accounts, which includes setting up accounts, changing passwords, allocating roles, and removing access.
   - They have the ability to set up system-wide parameters like storage rules, access control methods, and third-party tool integrations.
   - Administrators are in charge of security enforcement, which includes keeping track of audit logs, managing encryption keys, and making sure that legal or regulatory requirements are met.

Role Management Considerations

The following factors are essential to take into account when implementing user roles:

- Principle of Least Privilege: Each role only gives the bare minimum of permissions required by the principle of least privilege. A Viewer cannot inadvertently alter or remove data, for instance.
- Scalability: Without requiring a significant redesign, the model ought to accommodate future role expansions like Auditor, Super Admin, or Guest.
- Security: Only a select few reliable users should have administrator privileges. For auditing purposes, all role assignments and modifications must be recorded.

- Simplicity: Early on, roles should not be overly complicated hierarchies; instead, they should be simple to comprehend and manage.

Expected Outcome

The system guarantees a distinct division of duties by establishing these roles. Administrators have complete control over users and system operations, editors can add content and make updates, and viewers can access information safely. This method lowers errors, increases security, and lays a scalable basis for future access control expansion.

References

Frontegg. (n.d.). User role and permission guide. Frontegg. https://frontegg.com/guides/user-role-and-permission

IBM. (n.d.). What is role-based access control (RBAC)? IBM. https://www.ibm.com/think/topics/rbac

P. S. Anna. (2022, August 9). Best practices for managing users, roles, and permissions. Dev.to. https://dev.to/anna_p_s/best-practices-for-managing-users-roles-and-permissions-5140