# Roles (Public)

In **Keeper**, Roles are used to define permissions and security policies for users within an organization. They help administrators control access, enforce security measures, and streamline account management. Here's how Roles work within Keeper:

## Key Features of Roles in Keeper

1. **Permission Management** – Roles allow admins to assign different levels of access to users, controlling what they can view or modify within Keeper.
2. **Security Policies** – Roles can enforce security requirements such as multi-factor authentication (MFA), password complexity rules, and session timeouts.
3. **Delegated Administration** – Admins can create hierarchical roles, giving team leaders or IT personnel specific admin capabilities without granting them full system control.
4. **Shared Folders & Record Management** – Roles can define who can create, edit, and share records or folders within Keeper's vault.
5. **Auditing & Compliance** – Admins can track activity and enforce policies across different roles to meet compliance requirements.

## Common Role Examples

- **Super Admin** – Full control over all settings, users, and security policies.
- **IT Admin** – Manages user accounts, permissions, and integrations but may have limited access to stored records.
- **Team Manager** – Can manage user access within their department or project.
- **User** – Standard access to their Keeper Vault with permissions based on policies set by admins.

# Best Practice

## **1.** Use the Principle of Least Privilege

Assign users only the permissions they need to perform their tasks. Avoid giving broad administrative access unless absolutely necessary.

## **2.** Create Roles Based on Job Functions

Define roles based on user responsibilities, such as:

- **IT Admins** – Full access to user and security management.
- **Team Managers** – Limited user management within their department.
- **Standard Users** – Access to their personal vault and shared team folders.

## **3.** Enforce Security Policies Through Roles

- Require **multi-factor authentication (MFA)** for all sensitive roles.
- Set **session timeout policies** to prevent unauthorized access.
- Restrict access by **IP address or device type**, if necessary.

## **4.** Use Role-Based Access for Shared Folders

Instead of assigning permissions individually, manage shared records and folders through roles. This ensures consistent access control and simplifies administration.

## **5.** Implement a Role Hierarchy for Delegated Administration

If you have a large organization, create a hierarchy where:

- Super Admins oversee everything.
- Department-level admins manage their teams.
- Users have limited, controlled access to shared data.

## **6.** Review Roles Regularly

Periodically audit role assignments to remove outdated or unnecessary access. This helps prevent privilege creep and strengthens security.

## **7.** Test New Roles Before Assigning Them Broadly

Before rolling out a new role, test it with a small group to ensure permissions and restrictions work as intended.

# Example Role Structure

## **1.** SME Owner / Executive (Limited Admin Access)

- **Purpose:** The business owner or key executive who may need visibility but does not manage licenses or users.
- **Permissions:**
  - View security policies
  - Access company-wide shared folders
  - Cannot add/remove users or licenses
  - Cannot change billing settings

---

## **2.** IT / Security Champion (Internal Keeper Admin - Optional)

- **Purpose:** A designated employee responsible for enforcing internal Keeper policies (if the SME wants an internal point of contact).

- **Permissions:**
  - Manage user roles within the SME
  - View security audit logs
  - Reset user accounts (password rotation)
  - Cannot add/remove licenses or users

---

## **3.** Team Manager

- **Purpose:** Department heads or managers who need access to specific shared folders but have no administrative privileges.
- **Permissions:**
  - Manage and share records within assigned shared folders
  - Edit permissions for team members (within their department)
  - Cannot manage users or roles
  - Cannot change security policies

---

## **4.** Standard User

- **Purpose:** Regular employees who need access to the Keeper vault for company credentials.
- **Permissions:**
  - Access and store passwords in personal vault
  - Access assigned shared folders
  - Cannot create new roles or modify settings
  - Cannot share records outside the company

---

## **5.** Finance / HR User (Special Access Role - Optional)

- **Purpose:** Employees with access to financial or HR-related credentials that require additional security.
- **Permissions:**
  - Access only specific shared folders (e.g., finance records, payroll login details)
  - Enforced multi-factor authentication (MFA)
  - Cannot manage user roles or settings

---

# Additional Notes

- **Globe2 manages all licenses, user provisioning, and global security settings**, so **no SME user can add or remove licenses**.
- **Shared folders** should be structured by department (e.g., "Marketing Credentials," "Finance Logins") to prevent unnecessary access.
- **Audit logs and activity tracking** can be enabled for compliance and security monitoring.

Revision #4
Created 16 March 2025 19:39:23 by Doug
Updated 24 March 2025 14:55:52 by Doug