Access Granted

Securing Investigations with Role-Based Access Control (RBAC): The foundation for data integrity, evidence handling, and system security in professional investigation platforms.

The Risk of Unchecked Access

Without robust access controls, sensitive case data is vulnerable to unauthorized viewing, modification, or deletion, compromising investigations and violating legal thresholds.

Data Breach

Unauthorized users viewing confidential case files, PII, or victim information.

Evidence Tampering

Malicious or accidental alteration of evidence logs, notes, or Chain of Custody records.

Data Deletion

Irreversible loss of critical case information due to insufficient permissions.

The RBAC Principle: Access Through Roles

RBAC simplifies security by granting access based on a user's job function (Role), not their individual identity. Permissions are tied to the Role, not the User.

User → **Role** (e.g., Investigator) → **Permissions** (e.g., View Case, Edit Evidence) → **Resource**

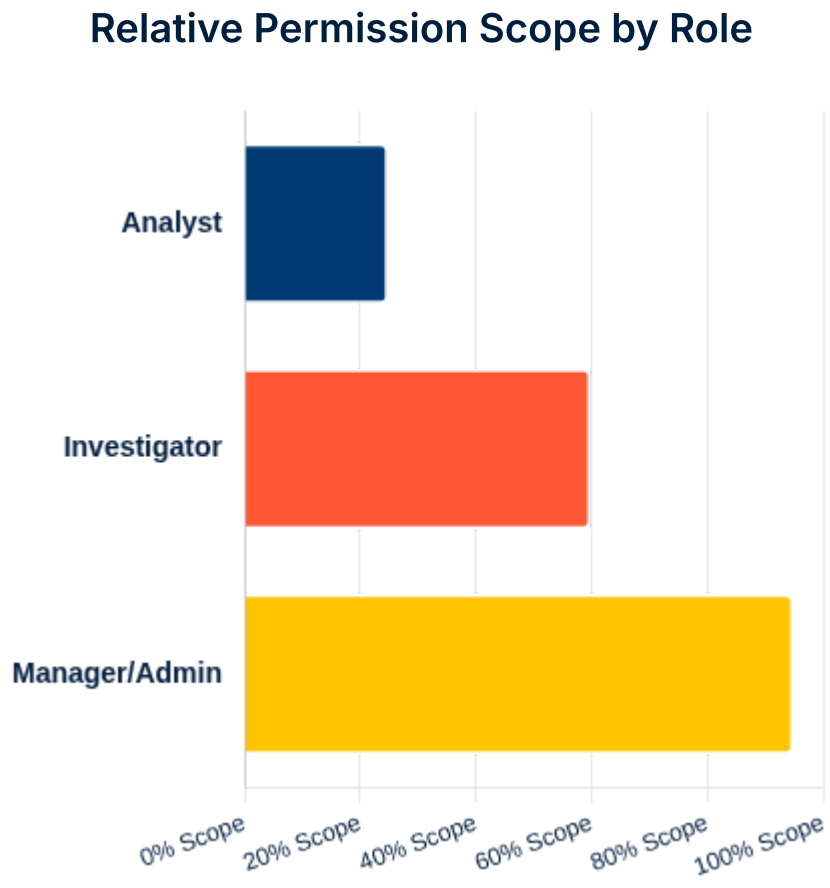
Defining Key Investigative Roles

Each role must have a clearly defined set of permissions that grants the minimum access necessary to perform their job (Principle of Least Privilege). Overly broad permissions create unnecessary risk.

Analyst: Focuses on data review and reporting. Needs read-only access primarily.

Investigator: Manages cases, collects evidence, conducts interviews. Needs read/write access to case data.

Manager/Admin: Oversees operations, assigns cases, manages users. Needs broader administrative permissions.



RBAC Implementation Flow

Implementing RBAC is a continuous cycle of definition, assignment, technical enforcement, and auditing.

1. Define Roles

Collaborate with stakeholders (Manny Method) to clearly map job functions to distinct system roles.

2. Assign Permissions

Grant specific permissions (Read, Write, Delete, Share) for each data type (Case, Evidence) to each Role.

3. Implement (Tina Toggle)

Configure the software (CaseBunker) to enforce these role-permission mappings technically.

4. Audit (Logan Logger)

Regularly review access logs to verify controls are working and detect unauthorized attempts.

The Importance of Auditing

RBAC defines the rules, but audit logs prove they are being followed. Comprehensive, immutable logs are essential for data integrity, legal compliance, and detecting insider threats.

70%

Reduction in unauthorized access incidents reported by organizations with robust RBAC and auditing.

Infographic generated from Knowledge Article KA-MOD-026. This visualization does not use Mermaid JS or SVG graphics.