```
users(
	id INTEGER PRIMARY KEY,
	first_name TEXT NOT NULL,
	last_name TEXT NOT NULL,
	username TEXT NOT NULL UNIQUE,
	email_address TEXT NOT NULL,
	password TEXT NOT NULL,
	salt TEXT NOT NULL,
	user_group TEXT NOT NULL
);

logs (
	log_time TEXT NOT NULL DEFAULT( STRFTIME('%Y-%m-%d %H:%M:%f', 'now')),
	event TEXT NOT NULL,
	username TEXT NOT NULL,
	filename TEXT
);

docs
(
	filename TEXT PRIMARY KEY,
	owner TEXT NOT NULL,
	body TEXT NOT NULL
);

doc_groups
(
	filename TEXT,
	doc_group TEXT NOT NULL
);
```

The users table is the central part of the system that stores information about user accounts and ensures secure authentication. The critical details include first and last names, unique usernames, and email addresses, which collectively help in identifying and contacting the users. Security has been kept foremost, and the password is stored encrypted with a unique salt to enhance protection against unauthorized access. Moreover, the user_group field allows for role-based access control, whereby a system can distinguish between an administrator, an editor, and a viewer. This makes the system adaptable to various user roles and responsibilities. This table ensures that the system is secure and scalable to meet the demands of diverse user bases.

The logs table plays a very important role in audit trailing, where the activities conducted by the users within the system are tracked. It captures the timestamp of every action-log_time, the

nature of the event-event, and the user responsible-username-with an optional filename field to link actions with specific documents. This provides greater transparency and accountability, recording in detail interactions with the system. Logs are extremely useful in terms of operational insight, such as usage pattern analysis, diagnosis, and compliance monitoring with organizational policies. This table becomes the cornerstone of system reliability since specific actions can be traced back to a particular user or document.

The docs table stores documents and their metadata in a centralized manner. It includes a filename as the primary key to uniquely identify each document, thereby avoiding any conflict or duplication. The owner field keeps track of who created the document or is the main person managing it, which gives clarity on responsibility and permissions. The body column contains the content of the document, which enables the basic functions of document creation, viewing, and editing. This table is important to the system for managing and retrieving documents efficiently and forms the basis for collaborative workflows.

The doc_groups table complements the document management system by associating documents with specific access or collaboration groups. The doc_group field will enable the grouping of documents according to projects, teams, or permissions for streamlined access control, enabling efficient organization of shared resources. This design supports diverse use cases, such as team-specific document collections, shared project files, or public access repositories. It lets the system uniformly enforce permissions with flexibility for different collaboration models by linking groups to documents.

These tables, taken together, form a coherent, integrated, and secure platform for managing users, tracking system activities, and organizing documents. The modular design means that each component plays a specific role while allowing for scalability and future enhancements. This architecture provides not only the support of current needs but also positions the system for growth and adaptability in a collaborative, document-driven environment.