Managing Users and Roles in Wazuh (v4.14+)

Wazuh operates on a **two-layered security model**. Because it is built on top of OpenSearch, user management is split into two parts:

1. **OpenSearch (Indexer):** Controls access to the underlying database and system settings.
2. **Wazuh App:** Controls access to security agents, rules, and dashboards.

To give a user full administrative privileges, you must grant them permissions in *both* layers. This guide outlines how to properly create an admin, how to assign restricted roles, and what those roles mean.

Part 1: How to Create a Super Admin User

Creating a Super Admin requires setting up the user in the Indexer, assigning them a specific "Backend role" to bypass system locks, and then mapping them to the Wazuh App.

Step 1: Create the User & Assign the Backend Role (Database Layer)

The **all_access** system role is locked by default. To make someone an admin, you must assign them the **admin** Backend Role, which automatically inherits full system access.

1. Click the **Global Menu (≡)** in the top left corner.
2. Navigate to **Indexer management** -> **Security**.
3. Click on **Internal users**, then click the blue **Create internal user** button.
4. Enter a descriptive **Username** and a secure **Password**.
5. Scroll down to the **Backend roles** section. Type `admin` into the box and click **Add another backend role** (or press Enter).
6. Click the blue **Create** (or Save) button at the bottom right.

Step 2: Map the User to the Wazuh App (Application Layer)

Now that the user has database access, you must grant them control over the Wazuh security features.

1. Click the **W. logo** in the top left to return to the Wazuh App.
2. Navigate to **Server management** -> **Security**.
3. Click the **Roles mapping** tab at the top of the screen.
4. Click the blue **Create Role mapping** button.
5. **Role mapping name:** Give it a recognizable name (e.g., *username_admin_access*).
6. **Roles:** Check the box for `administrator`.
7. Scroll down to the **Mapping rules** section. Under **Map internal users**, click the dropdown and select the user you created in Step 1.
8. *Crucial:* If there is a default "Custom rule" (e.g., one that looks for the word "wazuh"), click the **red trash can icon** to delete it.
9. Click **Save role mapping**.

The user is now a full Super Admin and can log in with total system control.

Part 2: How to Assign Standard Roles (e.g., Read-Only)

If you want to create a restricted user (like a junior analyst who can only view alerts but cannot change settings), the process is nearly identical, but you skip the `admin` backend role.

1. **Create the User:** Go to *Indexer management* -> *Security* -> *Internal users* and create the user. **Do not** add anything to the "Backend roles" section. Just save the username and password.
2. **Map the Role:** Go to *Server management* -> *Security* -> *Roles mapping* and click **Create Role mapping**.
3. **Select the Restricted Role:** In the Roles dropdown, select a restricted role like `readonly` instead of administrator.
4. **Map the User:** Select your new user from the "Map internal users" dropdown, delete any default custom rules, and save.

Understanding Built-In Roles

Wazuh comes with several pre-configured roles that dictate what a user can see and do within the application.

- **administrator:** Full control. The user can deploy agents, edit configuration files, create custom security rules, and manage other users.
- **readonly:** View-only access. The user can look at security events, read dashboard metrics, and check agent status, but cannot modify rules or system settings.
- **agents_admin:** Agent management only. The user can deploy, group, and manage endpoints, but cannot change core server configurations or indexer settings.
- **agents_readonly:** Granular view access. The user can only view data and alerts coming from the agents, without access to administrative menus.

> **Note:** Always ensure that users requiring global server configuration access are granted the `admin` Backend Role in the Indexer management menu, as Wazuh App roles alone cannot override database-level restrictions.

Revision #1
Created 2026-03-28 02:16:16 UTC by Francis
Updated 2026-03-28 02:17:13 UTC by Francis