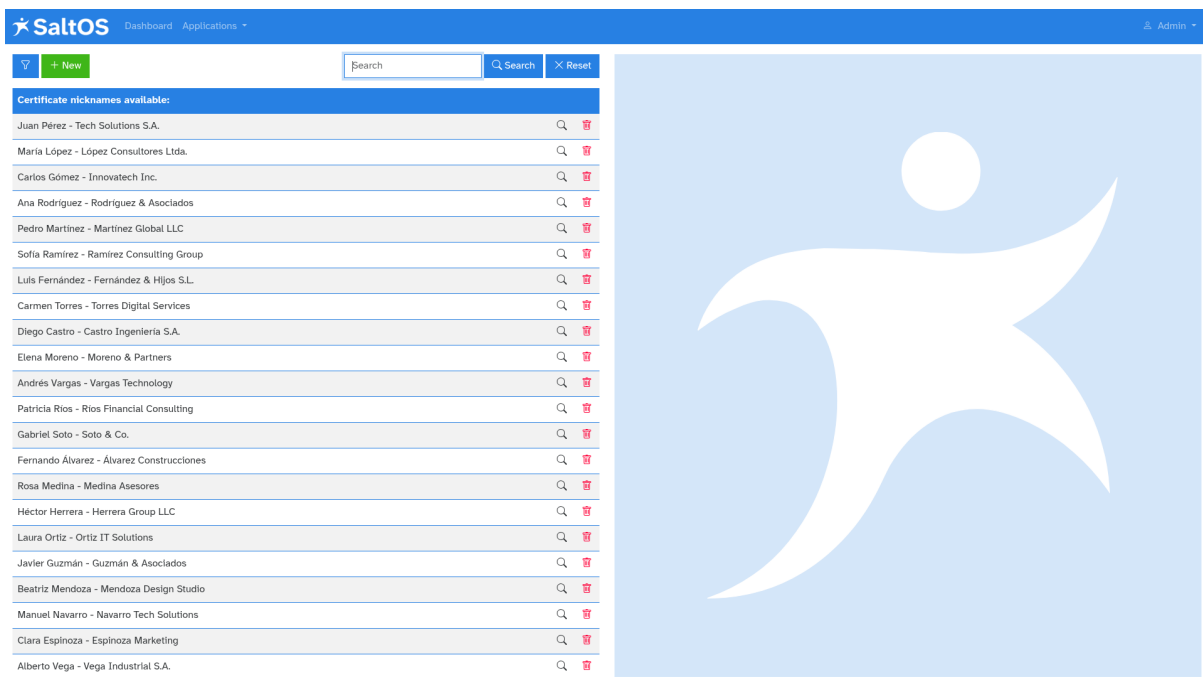# Certificates

Description

The Certificates application is used to manage and track SSL/TLS certificates stored or monitored by the system. This module allows administrators to register certificates, store metadata, monitor expiration dates, and ensure that security infrastructure remains up-to-date.

It is especially useful for managing certificates for custom domains, internal services, or external integrations.

List view

The following fields are displayed in the list view:

- Domain: Domain or hostname the certificate applies to.
- Type: Certificate authority or format (e.g., Let's Encrypt, Self-signed).
- Expiration: Date the certificate will expire.
- Status: Current state (Valid, Expiring Soon, Expired).
- Notes: Internal notes about the certificate.

Form view

This view is used to add, review, or update certificate information.

In **create** mode, the form is empty and ready to enter new data.

In **view** mode, the fields are filled with the selected record and cannot be edited.

The form includes the following fields:

- Domain: FQDN or hostname secured by the certificate.

- Type: Source or authority that issued the certificate.

- Expiration: Date on which the certificate will expire.

- Status: Optional status (may be auto-calculated).

- Certificate: Full certificate content (PEM, CRT, etc.).

- Notes: Remarks about usage or renewal schedule.

- Active: Indicates whether the certificate is currently monitored.

Delete

Certificates can be deleted if no longer relevant.

However, it is recommended to retain expired entries for audit purposes.