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



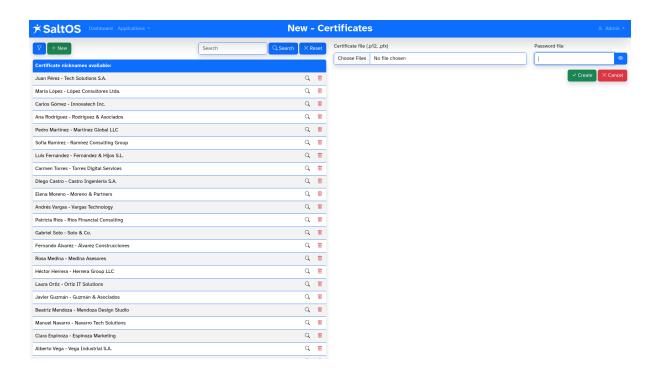
The following fields are displayed in the list view:

• Certificate nicknames available:: List of certificate aliases already stored and available in the system. It is not a database-driven table, but a visual display of loaded certificates.

Form view

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

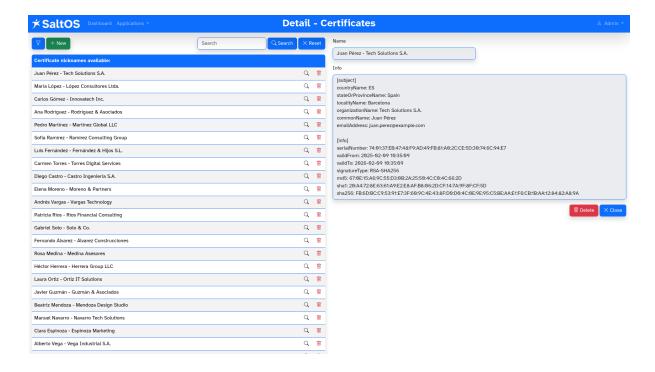
In create mode, the form is empty and ready to enter new data.



The form includes the following fields:

- Certificate file (.p12, .pfx): File input used to upload one or more certificates in PKCS#12 format. Required to import certificates into the system.
- Password file: Password used to decrypt the uploaded certificate file. This field is required and not autofilled for security reasons.

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



The form includes the following fields:

- Name: Display name or alias of the certificate.
- Info: Technical details of the certificate, including issuer, expiration, and subject. Displayed in a readonly text area.

Delete

Certificates can be deleted if no longer relevant.

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