Certificate management

The dashboard includes a **Certificates** section to import, view, and delete certificates. Clicking a certificate row opens the certificate editor.

Certificates list

Certificates are displayed in a sortable, paginated table. The list includes both client certificates and Certificate Authorities (CA).

Filters

At the top of the page you can enable filters using the chip list. Some filters are mutually exclusive.

- **All**: show all certificates.
- **Client**: show client certificates only.
- **Certificate Authority (CA)**: show CA certificates only.
- **Search**: shows a text field (label **Name or filename**) to search by certificate name or imported filename.
- **Without user**: show client certificates not associated with any user.

Table columns

- **Name**
- **Type**
- **Expiration**
- **User** (shown for client certificates)
- **Imported filename**
- **Import date**

Actions

- **Open certificate**: click a row to open the certificate editor.
- **Delete certificate**: available only when the certificate is not associated with users/policies and is not used by devices. The action can also be disabled when the license is expired.

- **Multi-row selection**: you can enable multi-row selection to delete multiple certificates at once. Only deletable certificates can be selected.
- **Refresh**: reload the certificates list.

Import certificates

To import certificates, click **Import certificate** and select one or more files. Supported formats are shown in the tooltip of the import button.

Clients

Supported format: Base64-encoded PKCS#12 (.p12 / .pfx).

Client certificates identify a user or a device on the enterprise network. Client certificates can be associated with a specific user.

Each client certificate can be optionally assigned to a specific user: this allows deploying the same Wi-Fi EAP configuration on many devices. You can do that in the policy's network configuration section, using the **EAP credentials from users** option.

> Alternatively, you can assign a certificate to a user from the **Users** page.

On Apple devices, certificates are installed with the **Networking** section of the Apple policy, where you can also choose **The certificate of the device user**. See the Networking page of Apple policies.

Certificate Authorities (CA)

Supported formats: Base64-encoded X.509 (.crt / .pem / .cer / .der).

CA certificates identify a Certificate Authority and indicate to the device that any certificates issued by the CA should be trusted. The dashboard validates that an imported X.509 certificate is a CA.

Certificate editor

When you open a certificate, the editor shows its main fields and a read-only **Certificate information** panel.

Main fields

- **Name** (required)
- **Id** (read-only)
- **Type** (read-only)
- **Expiration** (read-only)
- **Import date** (read-only)
- **Imported filename** (read-only)

User association (client certificates)

For **Client** certificates, the editor shows a **User** field. If a user is assigned, a menu allows you to **Open user**, **Change user**, or **Disassociate user**. If no user is assigned, you can assign one using the user action button.

Delete certificate

The delete action is disabled when the certificate is currently associated with a user or used in policies. It can also be disabled when the license is expired.

Revision #75
Created 2022-03-30 15:30:28 UTC by Admin
Updated 2026-11-12 09:51:52 UTC by Admin