Gestión de certificados

El panel de control incluye una sección **Certificados** para importar, ver y eliminar certificados. Si haces clic en una fila de certificado, se abre el editor de certificados.

Lista de certificados

Los certificados se muestran en una tabla ordenable y paginada. La lista incluye tanto certificados de cliente como autoridades de certificación (CA).

Filtros

En la parte superior de la página puedes activar filtros con la lista de chips. Algunos filtros son mutuamente excluyentes.

- **Todos**: muestra todos los certificados.
- **Cliente**: muestra solo los certificados de cliente.
- **Autoridad de certificación (CA)**: muestra solo los certificados de CA.
- **Buscar**: muestra un campo de texto (etiqueta **Nombre o nombre de archivo**) para buscar por nombre de certificado o nombre de archivo importado.
- **Sin usuario**: muestra los certificados de cliente no asociados a ningún usuario.

Columnas de la tabla

- **Nombre**
- **Tipo**
- **Vencimiento**
- **Usuario** (se muestra para certificados de cliente)
- **Nombre de archivo importado**
- **Fecha de importación**

Acciones

- **Abrir certificado**: haz clic en una fila para abrir el editor de certificados.
- **Eliminar certificado**: solo está disponible cuando el certificado no está asociado a usuarios ni políticas y no lo usan dispositivos. La acción también puede deshabilitarse

cuando la licencia está caducada.
- **Selección de varias filas**: puedes activar la selección de varias filas para eliminar varios certificados a la vez. Solo se pueden seleccionar los certificados que se pueden eliminar.
- **Actualizar**: vuelve a cargar la lista de certificados.

Importar certificados

Para importar certificados, haz clic en **Importar certificado** y selecciona uno o varios archivos. Los formatos admitidos se muestran en la información sobre herramientas del botón de importación.

Clientes

Formato admitido: PKCS#12 codificado en Base64 (.p12 / .pfx).

Los certificados de cliente identifican a un usuario o a un dispositivo en la red de la empresa. Los certificados de cliente se pueden asociar a un usuario concreto.

Opcionalmente, cada certificado de cliente se puede asignar a un usuario concreto: esto permite desplegar la misma configuración Wi-Fi EAP en muchos dispositivos. Puedes hacerlo en la sección configuración de red de la política, con la opción **Credenciales EAP de los usuarios**.

> También puedes asignar un certificado a un usuario desde la página **Usuarios**.

En los dispositivos Apple, los certificados se instalan con la sección **Redes** de la política de Apple, donde también puedes elegir **El certificado del usuario del dispositivo**. Consulta la página Redes de las políticas de Apple.

Autoridades de certificación (CA)

Formatos admitidos: X.509 codificado en Base64 (.crt / .pem / .cer / .der).

Los certificados de CA identifican a una autoridad de certificación e indican al dispositivo que debe confiar en los certificados emitidos por esa CA. El panel de control comprueba que un certificado X.509 importado sea una CA.

Editor de certificados

Cuando abres un certificado, el editor muestra sus campos principales y un panel **Información del certificado** de solo lectura.

Campos principales

- **Nombre** (obligatorio)
- **ID** (solo lectura)
- **Tipo** (solo lectura)
- **Vencimiento** (solo lectura)
- **Fecha de importación** (solo lectura)
- **Nombre de archivo importado** (solo lectura)

Asociación de usuario (certificados de cliente)

Para los certificados de tipo **cliente**, el editor muestra un campo **Usuario**. Si hay un usuario asignado, un menú te permite **Abrir usuario**, **Cambiar usuario** o **Desasociar usuario**. Si no hay ningún usuario asignado, puedes asignar uno con el botón de acción de usuario.

Eliminar certificado

La acción de eliminar está deshabilitada cuando el certificado está asociado actualmente a un usuario o se usa en políticas. También puede deshabilitarse cuando la licencia está caducada.

Revision #60
Created 2025-12-17 09:33:13 UTC by Admin
Updated 2026-11-12 09:54:26 UTC by Admin