

# Gerenciamento de certificados

O dashboard inclui uma seção de **Certificados** para importar, visualizar e excluir certificados. Clicar em uma linha de certificado abre o editor de certificados.

## Lista de certificados

Os certificados são exibidos em uma tabela paginada e classificável. A lista inclui tanto certificados de cliente quanto Autoridades Certificadoras (CA).

## Filtros

No topo da página, você pode ativar filtros usando a lista de chips. Alguns filtros são mutuamente exclusivos.

- **Todos**: mostra todos os certificados.
- **Cliente**: mostra apenas certificados de cliente.
- **Autoridade Certificadora (CA)**: mostra apenas certificados de CA.
- **Pesquisar**: mostra um campo de texto (rótulo **Nome ou nome do arquivo**) para pesquisar pelo nome do certificado ou nome do arquivo importado.
- **Sem usuário**: mostra certificados de cliente não associados a nenhum usuário.

## Colunas da tabela

- **Nome**
- **Tipo**
- **Expiração**
- **Usuário** (exibido para certificados de cliente)
- **Nome do arquivo importado**
- **Data de importação**

## Ações

- **Abrir certificado:** clique em uma linha para abrir o editor de certificados.
- **Excluir certificado:** disponível apenas quando o certificado não estiver associado a usuários/políticas e não for usado por dispositivos. A ação também pode ser desativada quando a licença estiver expirada.
- **Seleção de múltiplas linhas:** você pode ativar a seleção de múltiplas linhas para excluir vários certificados de uma só vez. Apenas certificados que podem ser excluídos podem ser selecionados.
- **Atualizar:** recarrega a lista de certificados.

## Importar certificados

Para importar certificados, clique em **Importar certificado** e selecione um ou mais arquivos. Os formatos suportados são exibidos na dica de ferramenta do botão de importação.

## Clientes

Formato suportado: PKCS#12 codificado em Base64 (.p12 / .pfx).

Certificados de cliente identificam um usuário ou um dispositivo na rede da empresa. Certificados de cliente podem ser associados a um usuário específico.

Cada certificado de cliente pode ser opcionalmente atribuído a um usuário específico: isso permite implantar a mesma configuração de Wi-Fi EAP em vários dispositivos. Você pode fazer isso na seção de [configuração de rede](#) da política, usando a opção de **credenciais EAP dos usuários**.

Como alternativa, você pode atribuir um certificado a um usuário na página de **Usuários**.

## Autoridades Certificadoras (CA)

Formatos suportados: X.509 codificado em Base64 (.crt / .pem / .cer / .der).

Certificados de CA identificam uma Autoridade Certificadora e indicam ao dispositivo que quaisquer certificados emitidos pela CA devem ser confiáveis. O dashboard valida se um certificado X.509 importado é uma CA.

## Editor de certificados

Quando você abre um certificado, o editor mostra seus campos principais e um painel de **Informações do certificado** apenas para leitura.

## Campos principais

- **Nome** (obrigatório)
- **ID** (apenas leitura)
- **Tipo** (apenas leitura)
- **Expiração** (apenas leitura)
- **Data de importação** (apenas leitura)
- **Nome do arquivo importado** (apenas leitura)

## Associação de usuário (certificados de cliente)

Para certificados de **Cliente**, o editor mostra um campo de **Usuário**. Se um usuário estiver atribuído, um menu permite **Abrir usuário**, **Alterar usuário** ou **Desvincular usuário**. Se nenhum usuário estiver atribuído, você pode atribuir um usando o botão de ação de usuário.

## Excluir certificado

A ação de exclusão é desativada quando o certificado estiver associado a um usuário ou sendo usado em políticas. Ela também pode ser desativada quando a licença estiver expirada.

---

Revision #49

Created 2025-12-17 09:34:33 UTC by Admin

Updated 2026-07-07 10:56:52 UTC by Admin