Gestione dei certificati

La dashboard include una sezione **Certificati** per importare, visualizzare ed eliminare i certificati. Facendo clic su una riga di certificato si apre l'editor del certificato.

Elenco dei certificati

I certificati sono visualizzati in una tabella ordinabile e paginata. L'elenco include sia certificati client sia Autorità di certificazione (CA).

Filtri

Nella parte superiore della pagina puoi abilitare i filtri usando l'elenco di chip. Alcuni filtri si escludono a vicenda.

- **Tutti**: mostra tutti i certificati.
- **Client**: mostra solo i certificati client.
- **Autorità di certificazione (CA)**: mostra solo i certificati CA.
- **Cerca**: mostra un campo di testo (etichetta **Nome o nome file**) per cercare per nome del certificato o nome del file importato.
- **Senza utente**: mostra i certificati client non associati ad alcun utente.

Colonne della tabella

- **Nome**
- **Tipo**
- **Scadenza**
- **Utente** (mostrato per i certificati client)
- **Nome file importato**
- **Data di importazione**

Azioni

- **Apri certificato**: fai clic su una riga per aprire l'editor del certificato.
- **Elimina certificato**: disponibile solo quando il certificato non è associato a utenti/policy e non è usato dai dispositivi. L'azione può anche essere disabilitata quando la licenza è

scaduta.
- **Selezione multipla**: puoi abilitare la selezione di più righe per eliminare più certificati contemporaneamente. È possibile selezionare solo i certificati eliminabili.
- **Aggiorna**: ricarica l'elenco dei certificati.

Importa certificati

Per importare i certificati, fai clic su **Importa certificato** e seleziona uno o più file. I formati supportati sono mostrati nel tooltip del pulsante di importazione.

Client

Formato supportato: PKCS#12 codificato in Base64 (.p12 / .pfx).

I certificati client identificano un utente o un dispositivo sulla rete dell'enterprise. I certificati client possono essere associati a un utente specifico.

Ogni certificato client può essere facoltativamente assegnato a un utente specifico: questo consente di distribuire la stessa configurazione Wi-Fi EAP su molti dispositivi. Puoi farlo nella sezione configurazione di rete della policy, usando l'opzione **Credenziali EAP dagli utenti**.

> In alternativa, puoi assegnare un certificato a un utente dalla pagina **Utenti**.

Sui dispositivi Apple, i certificati vengono installati con la sezione **Rete** della policy Apple, dove puoi anche scegliere **Il certificato dell'utente del dispositivo**. Consulta la pagina Rete delle policy Apple.

Autorità di certificazione (CA)

Formati supportati: X.509 codificato in Base64 (.crt / .pem / .cer / .der).

I certificati CA identificano un'Autorità di certificazione e indicano al dispositivo che qualsiasi certificato emesso dalla CA deve essere considerato attendibile. La dashboard verifica che un certificato X.509 importato sia una CA.

Editor del certificato

Quando apri un certificato, l'editor mostra i suoi campi principali e un pannello **Informazioni sul certificato** in sola lettura.

Campi principali

- **Nome** (obbligatorio)
- **ID** (sola lettura)
- **Tipo** (sola lettura)
- **Scadenza** (sola lettura)
- **Data di importazione** (sola lettura)
- **Nome file importato** (sola lettura)

Associazione utente (certificati client)

Per i certificati **Client**, l'editor mostra un campo **Utente**. Se è assegnato un utente, un menu ti consente di **Apri utente**, **Cambia utente** o **Disassocia utente**. Se non è assegnato alcun utente, puoi assegnarne uno usando il pulsante di azione utente.

Elimina certificato

L'azione di eliminazione è disabilitata quando il certificato è attualmente associato a un utente o usato nelle policy. Può anche essere disabilitata quando la licenza è scaduta.

Revision #8
Created 2026-11-10 15:12:48 UTC by Admin
Updated 2026-11-12 09:52:31 UTC by Admin