Gestione certificati

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

Elenco certificati

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

Filtri

Nella parte superiore della pagina è possibile abilitare i filtri utilizzando l'elenco di chip. Alcuni filtri sono mutuamente esclusivi.

- **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 tramite 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 dei certificati.
- **Elimina certificato**: disponibile solo quando il certificato non è associato a utenti/policy e non è utilizzato dai dispositivi. L'azione può anche essere disabilitata quando la licenza è scaduta.

- **Selezione multi-riga**: è possibile abilitare la selezione multi-riga 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 aziendale. I certificati client possono essere associati a un utente specifico.

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

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

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 tutti i certificati emessi dalla CA devono essere considerati affidabili. La dashboard convalida che un certificato X.509 importato sia una CA.

Editor dei certificati

Quando apri un certificato, l'editor mostra i suoi campi principali e un pannello di **Informazioni sul certificato** di 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 consente di **Apri utente**, **Cambia utente** o **Dissocia utente**. Se non è assegnato alcun utente, è possibile assegnarne uno tramite il pulsante delle azioni utente.

Elimina certificato

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

Revision #7
Created 2026-06-24 08:04:56 UTC by Admin
Updated 2026-06-24 09:39:21 UTC by Admin