

# Visualizza/Aggiungi certificato IPsec attendibile su router VPN RV320 e RV325

## Obiettivo

I certificati vengono utilizzati per verificare l'identità dell'utente su un computer o su Internet e per migliorare una conversazione privata o protetta. In RV320 è possibile aggiungere un massimo di 50 certificati tramite l'autofirma o l'autorizzazione di terze parti. È possibile esportare un certificato per un client o per un amministratore, salvarlo in un PC o in una porta USB e quindi importarlo. IPsec viene utilizzato per lo scambio di dati di generazione e autenticazione di chiavi, protocolli di definizione delle chiavi, algoritmi di crittografia o meccanismi di autenticazione per l'autenticazione e la convalida sicure delle transazioni online con certificati SSL.

In questo articolo viene illustrato come visualizzare e aggiungere un certificato IPsec attendibile sui router VPN serie RV32x.

## Dispositivi interessati

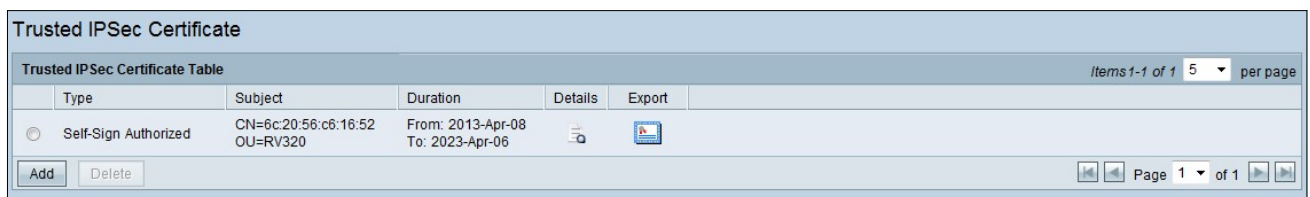
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router



## Versione del software

·v1.1.0.09

## Certificato IPsec attendibile

Passaggio 1. Accedere all'utilità di configurazione Web e scegliere **Gestione certificati > Certificato IPsec attendibile**. Verrà visualizzata la pagina *Certificato IPsec attendibile*:



Type	Subject	Duration	Details	Export
Self-Sign Authorized	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		

La pagina *Certificato IPsec attendibile* contiene i campi riportati di seguito.

- Tipo: sono disponibili due tipi di certificati
  - Autofirmato: è un certificato SSL (Secure Socket Layer) firmato dal proprio creatore. È meno affidabile in quanto non può essere annullato se la chiave privata è compromessa in qualche modo dall'autore dell'attacco.
  - Richiesta di firma certificata - Si tratta di un'infrastruttura a chiave pubblica (PKI) inviata all'autorità di certificazione per richiedere un certificato di identità digitale. È più sicuro della firma automatica in quanto la chiave privata viene mantenuta segreta.
- Oggetto: indica a chi viene rilasciato il certificato.

·Durata: indica la data di scadenza del certificato. La protezione del sito Web non può essere garantita se questa data è stata superata.

·Dettagli: mostra tutti i dettagli relativi all'autorità di certificazione, al numero di serie del certificato e alla data di scadenza generati dal servizio CA. Queste informazioni vengono utilizzate quando si crea una richiesta di generazione della firma del certificato e la si invia al servizio CA per la convalida.

·Esporta - Per esportare o visualizzare un certificato, fare clic sull'icona Esporta certificato. Viene visualizzata una finestra popup in cui è possibile aprire il certificato per l'ispezione o salvarlo su un PC.

Passaggio 2. Selezionare la casella di controllo **Abilita** per abilitare un certificato IPsec specifico.

Passaggio 3. Fare clic su **Add** per ottenere un nuovo certificato dal PC o dall'USB.

·Importa da PC: dal PC è possibile individuare il certificato e importarlo nel dispositivo

·Importa da USB: dall'USB collegato al dispositivo è possibile importare anche il certificato.

**Trusted IPsec Certificate**

3rd-Party Authorized

---

**Import Remote Certificate**

My Certificate : 01. Issuer : 6c:20:56:c6:16:52 ▼

Import from PC

Certificate:  Browse... ( PEM format )

Import from USB Device

USB Device Status: No Device Attached Refresh

Save Cancel

Passaggio 3. Fare clic su **Sfoglia** per individuare il certificato CA dal PC.

**Trusted IPsec Certificate**

3rd-Party Authorized

---

**Import Remote Certificate**

My Certificate : 01. Issuer : 6c:20:56:c6:16:52 ▼

Import from PC

Certificate: C:\CSR\MyCertWithKey.pem  ( PEM format )

Import from USB Device

USB Device Status: No Device Attached

Passaggio 4. Fare clic su **Salva** per aggiungere il certificato alla tabella dei certificati IPsec attendibili.