

# Visualizza/Aggiungi certificato SSL 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. RV320 consente di aggiungere un massimo di 50 certificati tramite autocertificazione o 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. SSL (Secure Sockets Layer) è la tecnologia di protezione standard per la creazione di un collegamento crittografato tra un server Web e un browser. Questo collegamento garantisce che tutti i dati trasferiti tra il server Web e il browser rimangano privati e integrali. SSL è uno standard di settore ed è utilizzato da milioni di siti Web per la protezione delle transazioni online con i propri clienti. Per poter generare un collegamento SSL, un server Web richiede un certificato SSL.

In questo articolo viene spiegato come visualizzare e aggiungere un certificato SSL attendibile sulla serie RV32x VPN Router.

## Dispositivi interessati

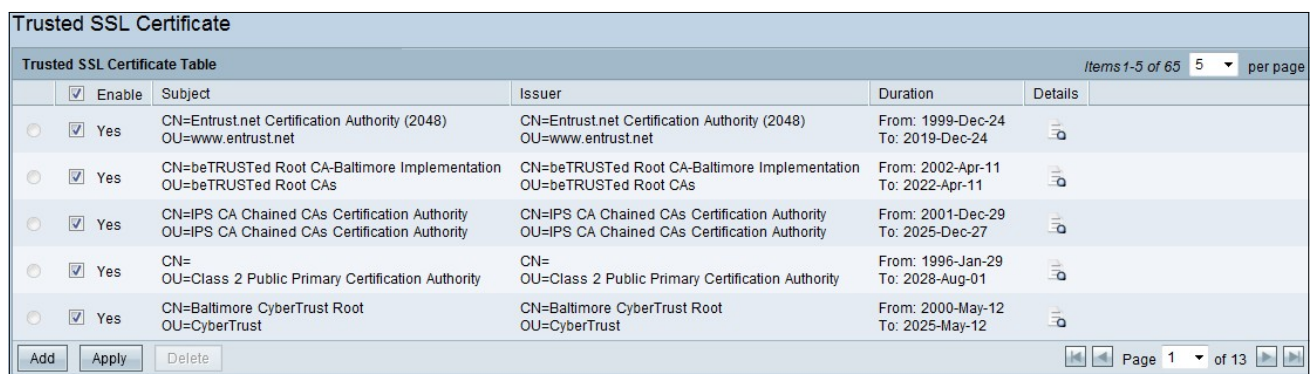
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

## Versione del software

·v1.0.1.17

## Certificato SSL attendibile

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



Trusted SSL Certificate					
Trusted SSL Certificate Table					
	Enable	Subject	Issuer	Duration	Details
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	CN=Entrust.net Certification Authority (2048) OU=www.entrust.net	CN=Entrust.net Certification Authority (2048) OU=www.entrust.net	From: 1999-Dec-24 To: 2019-Dec-24	
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	CN=beTRUSTed Root CA-Baltimore Implementation OU=beTRUSTed Root CAs	CN=beTRUSTed Root CA-Baltimore Implementation OU=beTRUSTed Root CAs	From: 2002-Apr-11 To: 2022-Apr-11	
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	CN=IPS CA Chained CAs Certification Authority OU=IPS CA Chained CAs Certification Authority	CN=IPS CA Chained CAs Certification Authority OU=IPS CA Chained CAs Certification Authority	From: 2001-Dec-29 To: 2025-Dec-27	
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	CN=OU=Class 2 Public Primary Certification Authority	CN=OU=Class 2 Public Primary Certification Authority	From: 1996-Jan-29 To: 2028-Aug-01	
<input type="radio"/>	<input checked="" type="checkbox"/> Yes	CN=Baltimore CyberTrust Root OU=CyberTrust	CN=Baltimore CyberTrust Root OU=CyberTrust	From: 2000-May-12 To: 2025-May-12	

Items 1-5 of 65 5 per page

Add Apply Delete Page 1 of 13

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

- Abilita - Indica se un certificato è abilitato o disabilitato.
- Emittente: fornisce le informazioni sull'emittente che rilascia il certificato

·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. Le informazioni vengono utilizzate quando si crea una richiesta di generazione della firma del certificato e la si invia al servizio CA per la convalida

Passaggio 2. Selezionare la casella di controllo **Abilita** per abilitare un determinato certificato SSL.

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 SSL Certificate**

3rd-Party Authorized

---

**Import SSL CA Certificate**

Import from PC

CA Certificate:   ( PEM format )

Import from USB Device

USB Device Status: No Device Attached

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

**Trusted SSL Certificate**

3rd-Party Authorized

---

**Import SSL CA Certificate**

Import from PC

CA Certificate:   ( 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 SSL

attendibili.